SECURING ACCESS TO WIRELESS LOCAL AREA NETWORKS USING A PASSIVE APPROACH TO DEVICE IDENTIFICATION

A Dissertation
Presented to
The Academic Faculty

by

Cherita L. Corbett

In Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy in the
School of Electrical and Computer Engineering

Georgia Institute of Technology
May 2006

SECURING ACCESS TO WIRELESS LOCAL AREA NETWORKS USING A PASSIVE APPROACH TO DEVICE IDENTIFICATION

Approved by:

Dr. John A. Copeland, Advisor
School of Electrical and Computer
Georgia Institute of Technology

Dr. George Riley
School of Electrical and Computer
Georgia Institute of Technology

Dr. Henry Owen
School of Electrical and Computer
Georgia Institute of Technology

Dr. Mustaque Ahamad
College of Computing
Georgia Institute of Technology

Dr. Chuanyi Ji
School of Electrical and Computer
Georgia Institute of Technology

Date Approved: April 4, 2006

To Isis

ACKNOWLEDGEMENTS

Words can not begin to express my gratitude to all those that were instrumental in my successful completion of the doctoral program. I know that I did not accomplish this alone and that it was the support, encouragement, and prayers of my family, friends, and colleagues that gave me the ability to stay the course and achieve my goals.

I would like to first thank a long time friend, Dr. Raheem A. Beyah for encouraging me to pursue a doctoral degree when I thought it was impossible. He continuously supported and guided me through this journey.

I would like to thank my advisor, Dr. John A. Copeland for providing guidance through my research endeavors and the freedom to foster my own research ideas. It was an honor to work with someone of his stature.

I am thankful to my thesis committee members, to my lab mates, Kathy Cheek, and the ECE administration. I would also like to thank all those that honored me with fellowships and scholarships that financially supported my education.

Last, but definitely not least, I would like to acknowledge my daughter, Isis. She served as my motivation during this entire process.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

SUMMARY

IEEE 802.11 wireless networks are plagued with problems of unauthorized access. Left undetected, unauthorized access is the precursor to additional mischief. Current approaches to detecting intruders are invasive or can be evaded by stealthy attackers. We propose the use of spectral analysis to identify the type of wireless network interface card (NIC). This mechanism can be applied to support the detection of unauthorized systems that use NICs which are different from that of a legitimate system.

We focus on two functions, active scanning and dynamic rate switching, required by the 802.11 standard that are implemented in the hardware and software of the wireless NIC. We show that the implementation of these functions influence the transmission patterns of a wireless stream that are observable through traffic analysis. Furthermore, differences in the behavior of a wireless stream caused by differences in the implementation of these functions are exploited to establish the identity of a NIC. Our mechanism for NIC identification uses signal processing to analyze the periodicity embedded in the wireless traffic caused by active scanning and rate switching. A spectral profile is created from the periodic components of the traffic and used for the identity of the wireless NIC. We show that we can discern between NICs manufactured by different vendors and NICs within the same manufacturer using the spectral profile.

1 INTRODUCTION

IEEE 802.11 wireless networks are plagued with problems of unauthorized access. Left undetected, unauthorized access is the precursor to additional mischief. Current approaches to detecting intruders are invasive or can be evaded by stealthy attackers. We propose the use of spectral analysis to identify the type of wireless network interface card (NIC). This mechanism can be applied to support the detection of unauthorized systems that use NICs that are different from that of a legitimate system.

Our approach to establishing the identity for different types of NICs focuses on the implementation of active scanning and rate switching, two functions required by the 802.11 standard. We show that differences in the implementation of these two functions cause unique traffic patterns that can be used to discern between NICs. We apply signal processing to analyze the periodicity embedded in the wireless traffic caused by active scanning and rate switching. A spectral profile is created from the periodic components of the traffic and used for the identity of the wireless NIC. We show that we can discern between NICs manufactured by different vendors and NICs within the same manufacturer using the spectral profile.

1.1 Contribution

We developed a mechanism for addressing the malleability of the identity of wireless network interface cards. Our technique passively analyzes the traffic patterns imposed by scanning and rate switching for the identification of a NIC. Therefore, the identity of a NIC is independent of any type of attack tool an intruder my use and does not rely on detection of alarming behavior (i.e., protocol abuse, violation of security

policy, jump in sequence number). Additionally, this allows the detection of authorized users with unauthorized wireless devices.

Furthermore, scanning and rate switching are two functions required by the 802.11 standard that are implemented in the hardware and software of a NIC. These functions are also used frequently by wireless clients. As a result, it is difficult to evade detection using our approach.

1.2 Organization

The remainder of this dissertation is organized as follows. Chapter 2 discusses the origin and history of the problem of unauthorized access and highlights related work. Chapter 3 discusses the composition of a wireless NIC and presents opportunities for distinguishing between different types of NICs. In Chapter 4, we present the rational for using signal processing and introduce our signal processing technique. We discuss how to represent a wireless traffic stream as a signal and how to compare spectral content. In Chapter 5, we use our technique to identify NICs during active scanning. In Chapter 6, we conduct an empirical analysis to characterize the rate switching phenomenon. We also conduct controlled experiments to show how rate switching impacts the periodicity of wireless traffic. Finally in Chapter 6, we conduct experiments that identify NICs in a real environment based on their implementation of the rate switching algorithm. Chapter 7 concludes the dissertation and discusses future work.

2 ORIGIN AND HISTORY OF PROBLEM

The 802.11 wireless local area networks (LANs) are plagued with problems of unauthorized access. Once hackers gain access, sensitive information can be stolen, network resources abused, or more sophisticated attacks can be launched targeting legitimate wireless devices or the Internet. Lack of physical boundaries and the use of an open-air medium make wireless networks an attractive target for malicious activity. As a result, wireless networks are easy to find and hackers only need to be within radio range to gain access.

This chapter discusses the evolution of the security flaws surrounding 802.11 wireless LANs to understand how the problem of unauthorized access currently exists. This chapter will also discuss existing preventive measures and detection techniques that seek to minimize the vulnerability of the wireless networks to unauthorized access.

2.1 Overview of 802.11 Security Flaws

IEEE 802.11 [1] specifies security services at the medium access control (MAC) layer that are intended to be equivalent to that provided by the physical security attributes inherent to wired LANs. The goals of the security services needed at the MAC layer include confidentiality, integrity, and access control. Confidentiality prevents eavesdropping and ensures only the intended audience understands the transmitted data. Data integrity prevents attackers from transparently modifying data and ensures the data comes from the source it purports. Access control, which is dependent on authorization and authentication, prevents unauthorized users from communicating on the wireless LAN.

The Wired Equivalent Privacy (WEP) protocol is the original security mechanism used by the IEEE 802.11 standard to enforce these security services [1]. The operation of the WEP protocol is based upon the RC4 cryptographic algorithm, the 32-bit cyclic redundancy code (CRC-32), and a secret key shared between communicating stations. Researchers have identified vulnerabilities in the WEP security mechanism that expose wireless LANs to serious intrusion risks. The remainder of this section will discuss the flaws of WEP in detail.

The RC4 algorithm is a critical component of the WEP design. As a stream cipher, a well-known pitfall of RC4 is that encrypting two messages under the same initialization vector (IV) and key, *k*, can reveal information about both messages.

If $C_1 = P_1 \text{ XOR } RC4(k,IV)$
and $C_2 = P_2 \text{ XOR } RC4(k,IV)$
then

$$C_1 \text{ XOR } C_2 = (P_1 \text{ XOR } RC4(k,IV)) \text{ XOR } (P_2 \text{ XOR } RC4(k,IV)).$$

$$= P_1 \text{ XOR } P_2.$$

Essentially, the exclusive-OR (XOR) operation on the two ciphertexts (C_1 and C_2) causes the keystream to cancel out leaving the XOR of the two plaintexts (P_1 and P_2). If an attacker knows a ciphertext, plaintext pair $<C_1,P_1>$ for a particular IV, then the attacker can derive the plaintext P_2 of other encrypted frames with the same IV without ever knowing the secret key. Researchers [3] [4] have demonstrated the practical keystream reuse attacks that allow eavesdropping.

In addition to the keystream reuse vulnerability, the authors of [6] revealed that there are patterns in certain IVs, called “weak IVs” that can be used to break the secret key. The authors illustrate that the RC4 key scheduling construct reflects patterns in keys themselves by producing patterns at the beginning of the generated keystream. All that is

needed is to recover the first byte of enough (100,000 to 1,000,000) encrypted frames that share the same secret key. Knowledge of the secret key reveals all encrypted communication to the attacker for the life of the key.

The implementation of data privacy in WEP depends on the ability to maintain the security of the keystream, which ultimately depends on the IV and secret key. The 802.11 standard recommends varying the IV per packet, but IV reuse is allowed. The 802.11 standard does not specify how to distribute keys. It relies on external key management services [1]. In practice, most installations use a single key for an entire network and very rarely change the key due to the administrative overhead. Poor key management and improper IV management help make the keystream reuse and weak IV exploit more practical.

The CRC-32 algorithm is used by WEP to protect the integrity of its frames. CRCs are good for detecting single random bit errors, but are not cryptographically secure. The CRC-32 checksum exhibits a linear property: CRC(A XOR B) = CRC(A) XOR CRC(B). This property allows an attacker to easily modify an encrypted frame without knowledge of the secret WEP key. To modify the encrypted packet, the attacker can XOR the original ciphered frame with the bit flip sequence and recalculate the integrity check value (ICV). The modified ciphertext C' becomes

$$
\begin{aligned}
C' &= C \ \text{XOR} \ [\Delta , \text{crc}(\Delta)] \\
&= \text{RC4}(k, IV) \ \text{XOR} \ [M , \text{crc}(M)] \ \text{XOR} \ [\Delta , \text{crc}(\Delta)] \\
&= \text{RC4}(k, IV) \ \text{XOR} \ [(M \text{ XOR } \Delta) , \text{crc}(M) \text{ XOR } \text{crc}(\Delta)] \\
&= \text{RC4}(k, IV) \ \text{XOR} \ [(M \text{ XOR } \Delta) , \text{crc}(M \text{ XOR } \Delta)] \\
&= \text{RC4}(k, IV) \ \text{XOR} \ [M' , \text{crc}(M')]
\end{aligned}
$$

The modified ciphertext, C', is valid, and after decryption, the modified message, M', would be accepted as valid because the CRC is correct. Packet modification can be

made to encrypted frames in transit without fear of detection. The attacker only needs to know the boundary of the ICV field [3]. The CRC checksum is not resilient enough against attacks that tamper with the contents of a frame.

In addition to the design flaws of WEP, its algorithm is only applied to the body of data frames. This means that the header of a data unit and the entire frame of management and control units are transmitted in the clear. An attacker can passively monitor the radio link to gather useful information about the network or record legitimate sessions to replay at a later time. The 802.11 standard does not offer a cryptographic message authentication code for any frame types to ensure frames originate from the source it purports to come from. Without message authenticity, attackers can inject constructed traffic to manipulate the wireless LAN. Furthermore, access control is hinged on the authenticity, integrity, and privacy of management frames to carry out the association and authentication process. With an attacker having the ability to eavesdrop and modify frames in transit, access control can be compromised [5]. To exacerbate the problem, the 802.11 standard only provides one-way authentication of the client to the access point. The absence of mutual authentication can be exploited to lure clients to an illegitimate access point.

2.2 Problem of Unauthorized Access

There are a myriad of attack tools (e.g., FakeAP, WEPCrack, Wellenreiter) [7] that exploit these flaws to passively and actively attack wireless LANs. Of particularly interest are attacks that result in unauthorized access. Unauthorized access is an attack whereby an illegitimate system injects traffic into the wireless network and the target network accommodates the new traffic. This type of attack can manifest itself as a denial

of service [8], a man-in-the-middle attack [9], a session-hijack or fraudulent use of the intended services offered by the wireless network (i.e., Internet, corporate services, etc.). Unauthorized access is feasible primarily because of the absence of cryptographic message authentication and the one-way authentication in the WEP access control mechanism. The risk of unauthorized access evolves from the attacker's ability to detect wireless LANs, sniff traffic, and extract credentials about the network. With this information, the attacker is able to masquerade as a client or an access point injecting 802.11 compliant frames into the network. The wireless network accommodates the frame since it has no mechanism for validating the origin, authenticity, or integrity of the frame. Once the attacker has circumvented the access control mechanism, more sophisticated attacks [10] can be launched to manipulate or disrupt the network.

Even in the presence of new security standards and intrusion detection systems, the problem of unauthorized access continues to evolve. Sophisticated attackers are able to use phishing techniques that lure an unsuspecting victim to divulge personal information. These credentials are used by the attacker to pose as an authorized user. Also, there is a growing concern for rogue systems exposing the wireless network to unauthorized access. Rouge systems are unsanctioned devices installed onto a managed network and are usually unsecured. Consider a scenario where an employee uses a personal laptop to access the corporate wireless LAN. The employee has the right credentials to access the network, but the personal laptop is an unauthorized device. This exposes the corporate wireless LAN to new risks, because the laptop may not have the latest patches and security protection and it may have pre-existing viruses. The corporate wireless LAN is also vulnerable to the wireless attacks that originate in the employee's

home. On the employee's home network, where access is less likely to be unprotected, there are opportunities of misuse by neighbors and by-passers. Some academic work has been to address rogue systems [11][12], but most solutions come from industry [13][14][15].

2.3 Intrusion Prevention

Reacting to the security weaknesses, the IEEE 802.11 standards committee sought to provide additional security features with the 802.11i specification [2]. 802.11i and the consortium variations solve the currently known security vulnerabilities of WEP, but new vulnerabilities are only a matter of time. To be effective, 802.11i requires new hardware and must be commonly applied to all systems on the wireless network. Consequently, the use of flawed legacy equipment will continue to be prevalent. In general, prevention mechanisms are only affective on systems that are owned, managed, and controlled by the network administrator. This method of defense cannot be enforced on rogue systems for which an administrator has no knowledge or control. Also, users may not enable any security measures.

2.4 Intrusion Detection

Despite new security enhancements, the risk of intrusion is still a legitimate concern because preventive measures may be circumvented, cost prohibitive, or not practiced at all. As a result, intrusion detection systems for wireless environments have emerged to detect unauthorized access. Detecting unauthorized access affords an opportunity to respond to the intrusion and curtail the potential damage to preserve the privacy and integrity of the network.

The author of [16] detects unauthorized access by identifying media access control (MAC) address spoofing. Many of the attack tools (e.g. FakeAP, AirJack, and Wellenreiter) aimed at obtaining unauthorized access rely on spoofing the MAC address of an authorized access point or legitimate client. The technique used in [16] monitors the sequence number field on the 802.11 frame header as a parameter to characterize normal behavior of a wireless LAN. The sequence number field is a sequential counter that is incremented by one for each non-fragmented frame. An attack is identified by a large gap in sequence numbers for an active MAC address. Additionally, if the sequence value increments sequentially with a changing source MAC address, BSSID, and SSID values, the behavior is also considered an attack. This technique can be evaded if the attacker is able to set the sequence number field to an arbitrary value. The approach also fails if the attacker uses a MAC address (authentic or spoofed) that has not previously been seen on the network. In general, signature-based techniques, such as this, require a continuous update of attack signatures to stay current. Further, this approach is not effective against novel attacks.

Commercial products, such as ReefEdge [17], AirDefense [18], and AirMagnet [19], offer a more comprehensive security solution with services for performance monitoring, intrusion detection, policy monitoring, and intrusion protection. AirDefense [18] is examined here to illustrate an anomaly-based approach to defending against unauthorized access. AirDefense uses a combination of attack signatures and policy compliance monitoring to identify threats and intrusions. The system dissects incoming traffic and attempts to match it to the behavior or pattern of known attack signatures. To address unknown attacks, policies are defined under four categories: configuration,

performance, vendor, and channel. The policies define limitations such as allowable channels of operation, allowable authentication modes, allowable data transmission rates, minimum signal strength, and approved vendor specific clients and access points (APs). AirDefense identifies an unauthorized system as one that violates the policies defined for a network. Using an anomaly approach driven by policy monitoring, the system is prone to many false positives. Alarms may be triggered because of a misconfigured end-user and not necessarily because of an intruder with unauthorized access. The AirDefense system consists of sensors and a server appliance. The sensor monitors the airwaves and transmits data to the server appliance, which analyzes the information and enforces the security rules. The number of sensors required grows with the number of APs in the network. The cost of additional hardware may cause this system to be impractical for some managed networks. AirDefense offers a gamut of services beyond security protection, such as reporting historical trends and network usage. To support these services, the sensors have to report detailed information gathered from the airwaves and communicate it to the server in a secure manner. The aggregation of this communication amongst multiple sensors imposes a heavy traffic load on the wired network.

Current wireless intrusion detection systems do not address stealthy intruders that do not exhibit anomalous behavior or generate a sequence of events matching the pattern of an attack. For example, a hacker may have obtained a user name and password from an authorized user via reconnaissance and phishing techniques. In which case, the attacker appears to have legitimate access and does not exhibit alarming behavior since it had the proper credentials.

2.5 Related Work

An alternative method to defending a wireless network from unauthorized access is to establish an identity for legitimate systems. Normally the MAC address of the network interface card (NIC) serves as a unique identifier. However, attackers can spoof the MAC address of legitimate devices. Authorized systems identified independent of their MAC address can be distinguished from intruders accessing the wireless network.

WiMetrics [20] is a commercially available monitoring and intrusion protection system. It implements an identity profiling process that can preauthorize a user through a registration process or authorize on the fly by probing the wireless device to derive an identity profile based on the response. Probing wireless stations is intrusive and as the number of clients increases, the already constrained network becomes burdened with additional traffic imposed by the system. This approach has other drawbacks including the administrative overhead of the preauthorization process. In addition, a hacker could elude the system by crafting responses to the probe request to impersonate the identity of a legitimate user, reducing the effectiveness of this scheme.

IPass Inc. developed DeviceID [21], a software-based authentication technology. DeviceID creates a digital fingerprint using random segments of serial numbers for different hardware components within the device. It consists of two components, server and client software. The server encrypts and inventories the digital fingerprint in a database. The client resides on all end-point devices to establish secure sockets layer (SSL) connections for secure transmission of the device's fingerprint required for hardware authentication. This approach is intrusive and suffers from administrative overhead involved in distributing the client software and updating the database every

time a hardware component changes in the device. Further, this approach generates traffic, placing additional strain on the wireless link.

Radio frequency fingerprinting captures the unique characteristics of the RF energy of a transceiver. When a radio transmitter is placed in transmit mode, a transient is generated by the frequency synthesizer whose function it is to generate the carrier frequency used for transmission. It has been determined that the turn-on transients generated are distinct enough that positive identification of the transmitter is possible. This technology was originally used in the cellular industry to identify fraudulent clones [22]. Researchers at Carleton University [23] have extended this approach to control access amongst BlueTooth wireless devices with future plans of including 802.11 transceivers. To implement this technology in a wireless LAN, special equipment for processing RF signals would be required at each access point. The cost of new equipment can become prohibitive especially for large networks with many access points. This was not of significant concern to the cellular industry because each tower services thousands of subscribers dissipating the cost of the equipment.

Kohno et al. [24] demonstrate a method for remotely fingerprinting a physical device by exploiting the implementation of the TCP protocol stack. When the TCP timestamp option is enabled, outgoing TCP packets reveal information about the sender's internal clock. The authors' technique exploits microscopic deviations in the clock skews to derive a clock cycle pattern as the identity for a device. For machines that do not enable the timestamp option by default, such as those running Windows 2000 and Windows XP, this approach becomes an active one. In such a case, the active fingerprinting technique initiates a connection and tricks the fingerprintee into using the

timestamp option. The active approach must violate the TCP specification in order to execute the trick. The drawback to the active technique is that it is detectable to the fingerprinted device. Furthermore, the entire approach only applies to TCP traffic and can be evaded by spoofing the TCP timestamp field or setting it to an arbitrary value.

3 WIRELESS NETWORK INTERFACE CARD

A wireless network interface card (NIC) is installed into a host to carry out the physical transmission of a packet over the air waves. To do so, the IEEE 802.11 specification requires the implementation of two layers: the physical (PHY) layer and the medium access control (MAC) layer. To support this implementation the NIC is organized into hardware, firmware, driver software, and utility software. The functions of 802.11 PHY are entirely implemented in hardware. The firmware is a microprogram semi-permanently embedded into ROM to control the hardware. It works to communicate between the hardware and driver software. Driver software accepts generic I/O commands from the OS of the host and then converts them into instructions the device can understand. The utility software is used to configure parameters to change the overall behavior of the hardware and software. The 802.11 MAC is implemented by a combination of hardware and software. The exact split is vendor specific and greatly impacts the performance of the NIC.

3.1 Opportunities for Distinction

The IEEE 802.11 standard specifies services that a wireless NIC must provide. However, the standard does not dictate how some of these services are to be implemented. It is left to the interpretation of the card manufacturer as to how to implement the 802.11 standard. We focus on the ambiguities in the 802.11 standard to differentiate between NICs manufactured by different vendors. This is analogous to operating system fingerprinting [25][26], which exploits differences in the implementation of the TCP/IP protocol stack to determine the type of an operating system.

To support the transmission of data packets and to cope with the changing conditions of a wireless environment, the 802.11 standard engages services such as: packet fragmentation, packet retransmission, adjusting transmission rates, reserving the link, probing network for connectivity, polling for packets to conserve power, etc. These services wield a certain behavior on the communication stream. This affords an opportunity to analyze properties about the stream, such as regularity in arrival rates and inter-arrival times of packets of different types and sizes. Cards with different implementations of the 802.11 standard will have a different impact on the time-variant properties of a wireless stream. We exploit this fact to identify NICs manufactured by different vendors. Specifically we hone in on the implementation of the scanning and rate switching mechanism to distinguish between NICs.

3.1.1 Scanning

Scanning is one of the primary 802.11 MAC functions, whereby a client seeks to discover available wireless networks to join. The standard [1] defines both passive and active scanning. In passive scanning mode, the NIC listens on individual channels for beacon frames from access points (APs), noting the corresponding signal strengths and other information about the access points. The NIC uses this information to decide which access point to use. Active scanning involves the broadcasting of probe request frames and the subsequent processing of received probe response frames. Active scanning enables a NIC to solicit an immediate response from an AP, without waiting on beacon transmissions. Active scanning is the default mode for NICs. For our research, we solely focus on active scanning, hereafter referred to as scanning.

The scanning mechanism is most often implemented in the device driver of the NIC. It is engaged when a NIC is first turned on as well as during a handoff procedure. A handoff is the change of AP to which a station is connected and occurs when the connection with the present AP degrades below a threshold. The guidelines set by the IEEE 802.11 MAC standard for the scanning procedure are as follows (modified for brevity):

For each channel to be scanned:

1) Wait until *ProbeDelay* time has expired.
2) Send a probe request with broadcast destination, SSID and broadcast BSSID.
3) Start a *ProbeTimer*.
4) If medium idle (i.e., there is neither a response nor any kind of traffic) when *ProbeTimer* reaches *MinChannelTime*, scan the next channel; else, when *ProbeTime* reaches *MaxChannelTime*, process all received probe responses and scan next channel.

ProbeDelay is the delay to be used prior to transmitting a probe request frame on a new channel. *MinChannelTime* is the minimum amount of time to spend on each channel. *MaxChannelTime* is the maximum amount of time to spend on each channel.

Recent research [27][28] has been done analyzing the scanning process for its impact on the handoff performance. Contributions have been made in developing new schemes that minimize the amount of time a NIC spends scanning. The authors noted that during their hand-off measurements, the scanning duration varied among cards by

different vendors. We exploit variations in the scanning mechanism to identify cards by different vendors.

The scanning procedure is vaguely specified, consequently forcing vendors to implement proprietary solutions. The scanning process has several parameters that can vary per vendor including:

- values for *ProbeDelay*, *MinChannelTime*, *MaxChannelTime*
- number of probe request frames to transmit per channel
- delay between probe request frames on the same channel
- channel probe frequency
- order of channels to probe

The performance of the scanning mechanism depends upon the setting of these parameters and defines the behavior of the wireless stream. We apply spectral analysis on the traffic stream to extract the traffic patterns imposed by the scanning mechanism to identify NICs by different vendors.

3.1.2 Rate Switching

Dynamic rate switching [1] is another important function of the 802.11 MAC and PHY. The 802.11 PHY has multiple data transfer rate capabilities that allow wireless cards to perform dynamic rate switching with the objective of improving performance. For example, 802.11b supports data transfer rates of 1, 2, 5.5, and 11 Mbps. Each rate corresponds to a different PHY modulation scheme with its own trade-off between data throughput and operating range. It is the responsibility of the rate switching algorithm to

select the proper rate (modulation scheme) per packet that gives maximum throughput for certain link conditions.

Like the scanning mechanism, implementation of the rate switching algorithm is vaguely specified by the 802.11 standard leading to vendor-specific solutions. Considering the sensitivity of intellectual property we cannot guarantee completeness of the review of rate switching algorithms. However, the literature survey [29][30][31][32] reveals three general approaches. Current WLAN products are believed to use a statistics-based feed-back approach to rate switching algorithms. Frame-error rate, achieved throughput, and acknowledged transmissions are used to estimate the quality of the link to select the appropriate rate for subsequent packet transmissions. The statistic-based approaches are outlined below.

3.1.2.1 Throughput-based

In throughput-based rate switching, a constant fraction of data is sent at two adjacent rates to the current rate. At the end of a specified window of time, the throughput at all rates is calculated as the ratio of number of bytes transmitted to cumulative transmission time. A switch is made to the rate that provides the highest throughput during the decision window. It is speculated that the Atheros WLAN card uses this approach in the Windows OS driver for 802.11a products based on the AR5000 chipset.

3.1.2.2 Frame-Error Rate

The Frame-Error Rate (FER) algorithm computes the ratio of received acknowledgement frames to the number of transmitted data frames during a specified window of time. If the ratio exceeds some threshold and the current rate is not the

minimal, then a switch is made to the next lower rate. Conversely, if the FER ratio is below a second threshold, probe the link at the adjacent higher rate with *n* frames. If all *n* frames sent at that probing rate are acknowledged, then switch to that rate. The length of the window and thresholds control the behavior of the FER control algorithm.

3.1.2.3 Autorate Fallback Algorithm

The Autorate Fallback Algorithm (AFR) is similar to FER in that it depends on acknowledged (ACK) frames. The protocol specifies that if ACKs for *n* consecutive data frames are not received by sender, then switch transmission rates to the next lower data rate and start a timer. If *m* consecutive ACKs are received, raise the transmission rate to the next higher data rate and cancel timer. Otherwise, when the timer expires raise the transmission rate. If an ACK is not received for the very next frame, lower the rate again and reset the timer. The AFR algorithm is believed to be used in Lucent's 802.11 WaveLan II card.

3.1.2.4 Retry-based

The retry-based approach to rate switching is broken into two stages to address short-term and long-term variations in channel conditions. For the first stage, there is an ordered set of 4 pairs of rate transmission count parameters {r0,c0}, {r1,c1}, {r2,c2}, {r3,c3}. Transmission of data starts at rate r0. If transmission fails, data is resent with rate r0 for c0-1 times. If transmission continues to fail, the algorithm tries rate r1, c1 times, then rate r2, c2 times, and finally rate r3, c3 times. Transmission is abandoned when the transmission has failed c0 + c1 + c2 + c3 times. In the second stage, the values for the 4 pair of parameters are changed at a regular fixed interval. The rate r3 is always chosen to be the minimum available rate. The rate r0 is determined from previous values of r0 and

the transmission results over an elapsed period of time. Rates r1 and r2 are determined by r0.

3.1.2.5 Summary

The rate switching algorithms described above each have a slightly different approach to estimating the channel quality and selecting a transmission rate. Each approach has a unique set of tunable parameters (i.e. threshold for losses, successes, and retries, duration of timers, etc.) that control how the algorithms respond to transient and long-term changes in the condition of the wireless channel. Thus, each will have a different impact on transmission duration, inter-packet delay, throughput capacity, occurrence of retransmissions, and other observable traffic characteristics. Additionally, differences in the setting of parameters within a particular algorithm will also display a distinguishable behavior.

All algorithms will have some form of the approaches highlighted above where they process frame transmission history to make a decision to switch rates. The agility of the rate switching algorithm determines how often the rate changes and to what rate it changes, which impacts the traffic pattern. Some algorithms may send more frames at a higher rate and fewer frames at a lower rate, or vice versa. The selection of the transmission rate can widen or reduce the inter-arrival time between data frames. The side effects of the rate switching algorithm not only impact the individual flow, but its effect is amplified within aggregate traffic as well. Research [33] has shown that the aggregate throughput declines and jitter and delay are compromised if at least one node in the network is performing rate switching. We investigate the periodicity imposed on the

wireless traffic by the rate switching algorithm. We look for distinctive spectral features to identify cards with different implementations of the rate switching algorithm.

3.1.3 Other Opportunities for Distinction

The 802.11 standard supports the dynamic configuration of the NIC to tune its behavior to be conducive to a variety of environments. Examples of configurable parameters include fragmentation threshold, request-to-send (RTS) threshold, transmit power, and power save mode. Different settings of these parameters can alter the behavior of traffic. For example, the RTS threshold sets the data packet size for which to invoke the request-to-send/clear-to-send (RTS/CTS) handshake to reserve the wireless link prior to data transmission. The RTS/CTS handshake is overhead that widens the inter-arrival time between data packets. A NIC with the RTS threshold set to a lower value will trigger the RTS/CTS handshake more frequently than a RTS threshold with a higher value. As a result, the packets' inter-arrival time would be larger and this phenomenon would occur more often than for the higher RTS threshold.

In addition to the basic services specified in the 802.11 standard, manufacturers often include acceleration hardware and software to increase performance gains and to support future standards prior to ratification. Enhancement techniques currently deployed to improve data transmission rates include data compression, frame bursting, overhead management, and client-to-client transfer **[34]**. The use of proprietary enhancement techniques can help to distinguish between devices. For example, the frame bursting technique, which is based on the proposed 802.11e standard, unpacks short data packets and rebundles them into a larger packet. A NIC with frame bursting technology would

exhibit different timing features by generating larger packets and less frequent management and control overhead traffic than a NIC without the service.

4 SIGNAL PROCESSING

The objective of our research is to show that it is possible to establish the identity of a wireless NIC by analyzing the temporal behavior of a wireless traffic stream. To achieve this objective we need an extensive level of detail about the dynamics of a wireless stream. In this chapter we present the rationale for applying spectral analysis, discuss signal representation of wireless traffic, explain the signal processing technique we use, and discuss how to compare spectral content.

4.1 Rationale for Spectral Analysis

To date, most of the analysis on the behavior of wireless networks have been geared towards understanding transmission rates, throughput, makeup of the composition of wireless stream (i.e., control traffic vs. data traffic), and the amount of overhead traffic. This type of analysis has been successfully done in the time domain using monitoring tools and network analyzers. However, we need a much more sophisticated technique to characterize time-variant details to capture the artifacts embedded in the stream such as those caused by vendor-specific implementations. We focus on the scanning and rate switching mechanisms required by the IEEE 802.11 standard.

Spectral analysis is a valuable tool for extracting timing information that may not otherwise be conveyed in the time domain. Spectral analysis is particularly useful in extracting periodic phenomena from (noisy) signals, because it succinctly compares the inter-relationship between all data points. In the context of a communication network, periodicity means that if we see a frame in the network, then chances are that after a constant period of time, we will see another packet passing through the same point. Networks inherently exhibit periodicity due to underlying protocols, network

components, or host machines. The IEEE 802.11 standard is no exception. For example, in the 802.11 distributed coordination function (based on the CSMA/CA protocol), every arriving data frame at the receiver allows the departure of an acknowledgement (ACK) frame, and every arriving ACK at the sender allows the injection of a new data frame. These exchanges must adhere to time specific inter-frame spacing consequently exhibiting periodicity (Figure 1). The same is true for other 802.11 functions. As expected, network contention and interference in a wireless network can impact the periodicity of the traffic stream. However, spectral analysis is resilient to noisy datasets in extracting timing information.

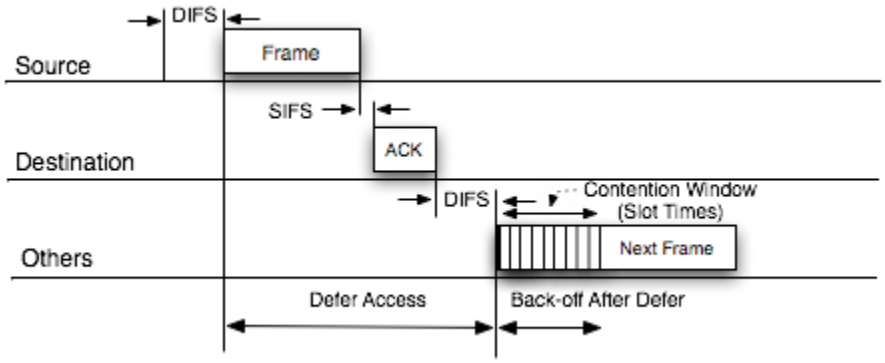


Figure 1 802.11 distributed coordination function

Spectral analysis has been shown to work well with identifying minute changes in the temporal behavior of network traffic. The authors of [35] applied spectral analysis to distinguish between normal TCP traffic and Denial-of-Service (DoS) attack traffic in aggregated, high-volume traffic. Hussain [36] extended on this work and showed that spectral analysis was useful in detecting the variations in the spectral profile attack stream as the composition (i.e., CPU speed, operating system, host load, etc.) of the attack host changed. This improved classification of the attacker beyond the type of

attack tool. Partridge [37] applied spectral analysis to wireless networks in order to deconstruct the traffic stream into individual flows, or sessions. Their results showed that they were able to successfully detect individual flows without hearing transmissions directly related to an individual flow.

We use spectral analysis to reveal differences in wireless streams generated by NICs that have different implementations of the 802.11 protocol. We specifically examine the spectral content of the active scanning mechanism within wireless cards manufactured by different vendors. We also examine how vendor-specific implementations of the rate switching algorithm impact the spectral content of a wireless stream.

4.2 Signal Representation

In order to apply spectral analysis, we need to represent a wireless stream of traffic as a signal that is suitable for the target signal processing function. The frame transmission process that occurs in WLANs can be described as a discrete event x, that occurs as a function of time t, that is $x(t)$. There are a multitude of time-varying signals that can be generated from WLAN traffic. Even with encrypted traffic, the 802.11 header offers a rich source of information for signal representation: size of frame, type of frame, direction of frame, duration of frame, transmission rate of frame, received signal strength of frame, etc.

Once the information has been chosen to be represented by the signal $x(t)$, the signal must be uniformly sampled. A general approach is to pick an appropriate interval T, bin time into increments at that interval (nT), and count the number of events that arrive during that bin of time $(t, t + T]$.

$$x(t) = x(nT) \quad \text{where } n = 0, 1, 2, 3, \ldots$$

The evenly spaced time interval T is called the sampling interval of the signal. The sampling frequency F_s is its reciprocal.

$$F_s = \frac{1}{T}$$

To determine the sampling frequency, the Shannon Sampling Theorem [38] states that to reproduce a signal with its highest frequency component F_{max}, the sampling frequency F_s must be at least twice F_{max} . This frequency is referred to as the Nyquist frequency F_c .

$$F_c \geq 2 \times F_{\max}$$

If the sampling frequency F_s is lower than the Nyquist frequency, the signal is undersampled. Undersampling causes energy at a frequency higher than half the sampling rate (F_s/2) to alias or fold back to a lower frequency, F_a [38]. It is important to account for this phenomenon when analyzing network traffic.

4.3 Power Spectrum Density

A common spectral analysis technique is the periodogram [39], or power spectrum density (PSD). A PSD captures the power or spectral density a signal has over a range of frequencies. The magnitude of the power indicates the amount of the regularity of the periodicity at the corresponding frequency. For our encoded wireless traffic signal, the PSD captures the periodicity in the arrival rate of frames. The magnitude corresponds to how often the arrival pattern occurs. PSDs are useful for identifying key frequencies to characterize the temporal behavior of a wireless stream.

4.3.1 Theoretical Description

A PSD compares the inter-relationship within a signal. It does so by using the discrete-time Fourier transform (DFT) of the samples of a signal and taking the magnitude squared of the result. The PSD P_{xx}, of a signal of length L is given as

$$\hat{P}_{xx}(f) = \frac{|X_L(f)|^2}{f_s L} \quad ,$$

where the discrete Fourier transform, X_L is given as

$$X_L(f) = \sum_{n=0}^{L-1} x_L[n] e^{-2\partial jfn/f_s} \quad ,$$

and x[n] is discrete sequence of events.

The DFT takes a time-series representation of a signal and maps it into a frequency spectrum. It is a decomposition of a function into harmonics of different frequencies.

4.3.2 Welch Method

During our analysis we used the Welch Average Periodogram method (provided by the Matlab Signal Processing Toolbox) to estimate the power spectrum density. The Welch method [40] is implemented as follows:

1) The input signal vector x is divided into k overlapping segments according to segment length l and number of overlapping samples *noverlap* .
2) The specified windowing function w is applied to each segment of x.
3) An *nfft*-point FFT is applied to the windowed data.
4) The modified periodogram of each windowed segment is computed.

5) The set of modified periodograms is averaged to form the spectrum estimate $\hat{P}_{xx}(f)$.

6) The resulting spectrum estimate is scaled to compute the power spectral density as $\hat{P}_{xx}(f)/F_s$, where F_s is the sampling frequency.

The number of segments k that x is divided into is calculated as:

$$k = \frac{(m-o)}{(l-o)}$$

In this equation, m is the length of the signal vector x, o is the number of overlapping samples (*noverlap*), and l is the length of each segment.

The Welch method returns the PSD vector and corresponding vector of frequencies. This is a measure of exactly what frequencies are present and at what magnitude. Averaging done in the Welch method reduces the influence of noise. Additionally, the smoothing done by the windowing function w reduces spectral background noise and clutter levels at the cost of some smearing of the peak energies in the frequency domain.

The Welch method depends upon several parameters: type of windowing function, segment size, number of data points to overlap between consecutive segments, and number of points for the FFT. The setting of these parameters affects the outcome of the Welch estimator. We discuss the significance of these parameters below.

4.3.2.1 Window

The window is a smoothing function that is time-wise multiplied with the signal. Popular choices for windowing include Hamming, Hanning, and Rectangular. When

considering a windowing function there is a trade-off between the main lobe width and side lobe height properties. The smaller the main lobe width, the better the resolution (or the narrower) of the peaks. Whereas, a high side lobe height, reduces the spectral leakage so spurious frequencies are less severe. Signals representing wireless traffic are usually noisy. Spectral leakage exacerbates the problem that noise causes in a signal, making real peaks indistinguishable from artificial peaks. Therefore we implemented the Hanning windowing function for its side lobe height. The trade-off is a loss in resolution. Spectral peaks will be wider, but distinguishable from the noise floor. The PSD resolution attainable with the Hanning window is ½ that attainable with a rectangular window (see Figure 2).

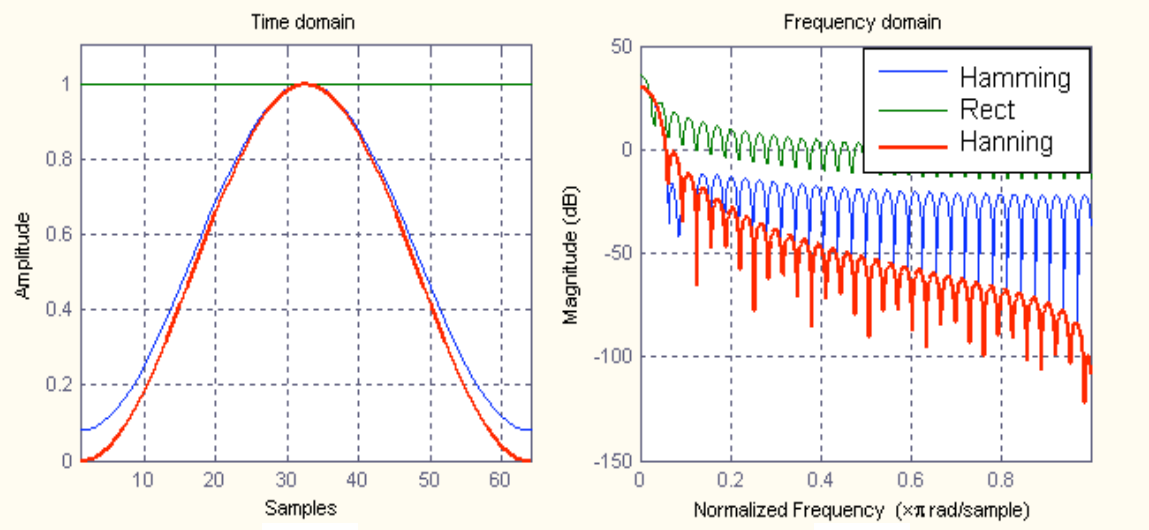


Figure 2 Illustration of popular windowing functions in the time and frequency domain

4.3.2.2 Segment Size

The choice of segment size also affects the resolution of the PSD. As the segment size decreases, the set of segments over which Welch does averaging increases. This in turn produces a smoother PSD, where peaks of the waveform become blunt and

sometimes disappear. On the other hand, an increase in segment length increases the frequency resolution. That is, the ability of the filter to separate very close frequencies in the signal. For traffic analysis, the length of the segment determines the type of statistical information portrayed in the PSD. The longer the segment length, the more the PSD is capable of depicting slow varying statistics revealing low frequency features. In contrast, smaller segments only capture signal statistics that vary quickly.

4.3.2.3 Noverlap

The *noverlap* determines the number of samples to overlap between consecutive segments. Overlapping segments causes additional averaging or smoothing of the PSD. For our analysis we overlap segments by 50%.

4.3.2.4 NFFT

The *nfft* parameter determines the number of FFT coefficients. The resulting PSD is represented by a vector with *nfft*/2 data points. The frequency range represented by each data point is $F_s/nfft$. It is a good rule of thumb to select *nfft* as a power of two to reduce computational complexity.

4.4 Comparing Spectra

Using the PSD estimator generates a spectrum of *nfft*/2 data points. It contains the magnitude of power at frequencies that are present in a signal. Ideally one would like to use the complete spectra for comparisons between different signals. However, this can be computationally expensive. Rather than using the complete spectra, we select a subset of PSD values to represent the key spectral features of the signal using the following algorithm:

Given a time series *x(t)*,

1. [Pxx, Freq] = PSD(x)	Estimate the PSD of *x(t)*, which returns a vector of frequencies *Freq* and a vector of power *Pxx* that corresponds to the frequencies.
2. [sorted_Pxx, IX] = sort(Pxx)	Sort the *Pxx* vector in descending order, which returns an array of indices *IX* of the elements in *Pxx* in descending order.
3. [sorted_Freq] = Freq(IX)	Use the indices of *IX* to match the ordering with the sorted vector of power sorted_Pxx.
4. spectral profile = sorted_Freq(1:N)	Use the first *N* values of the sorted frequency vector to constitute the spectral profile.

The algorithm above locates *N* frequency points that exhibit the greatest amount of power to constitute a spectral profile $F = \{f_1, f_2, f_3, \ldots f_{50}\}$. These key frequency points estimate the most prevalent arrival rates of frames in a wireless stream.

5 NIC IDENTIFICATION USING SCANNING

Recall from section 3.1.1 that scanning is the mechanism that NICs use to search for available wireless networks to join. The traffic generated during the scanning process presents itself as an opportunity for distinguishing between wireless NICs manufactured by different vendors. We have pinpointed this mechanism as an attribute within the NIC to identify cards manufactured by different vendors. The scanning process has several characteristics that vary per vendor including: 1) order of channel probing; 2) number of probes per channel; 3) frequency of probes per channel; 4) delay between probes on same channel; and 5) delay between probes on different channels. We apply our signal processing technique to capture the temporal behavior of the scanning process. In the following sections we explain the experimental setup, apply our spectral analysis technique, and evaluate the results.

5.1 Experimental Setup

For our experiments we used one access point, one client station to engage the scanning procedure, and three wireless sniffers collected traffic for analysis. Figure 3 illustrates the layout. All experiments were done in an isolated environment where there was little or no other wireless activity from neighboring networks.

5.1.1 Client Setup

We used a 1GHz Celeron Toshiba laptop with Linux Redhat 9 as the wireless client. Wireless cards interface with the laptop via the PCMCIA slot. We tested five different cards: two Lucent/Orinoco Gold cards, two Linksys WPC11 cards, and a D-Link DWL-650 card. During the experiments, the Lucent cards used the *orinoco_cs* software driver. The Linksys and DLink cards used the *prism2_cs* software driver. The experiments were conducted in the following manner for each card. A card was inserted into the PCMCIA slot and ejected after 4 minutes expired. The scanning process is

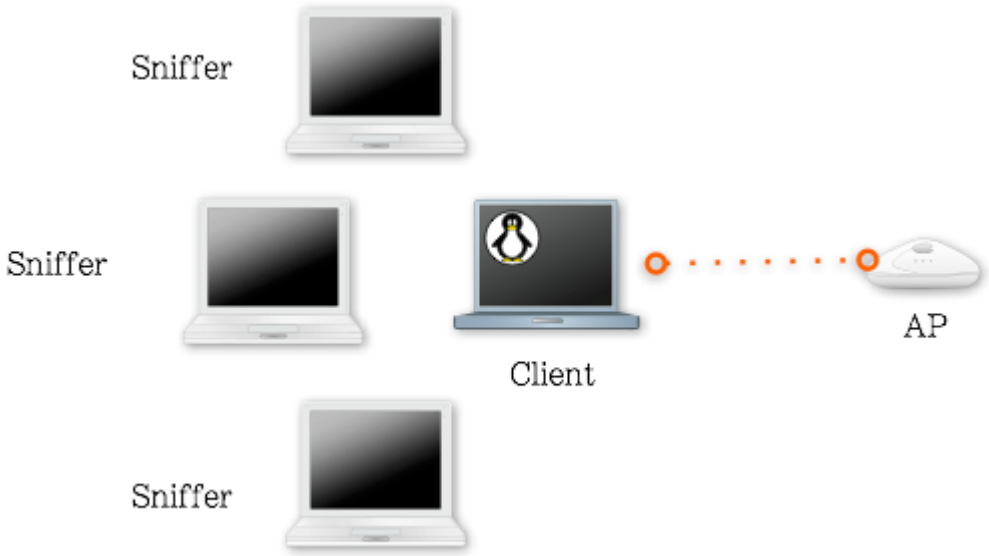


Figure 3 Experimental Setup

automatically engaged upon inserting the card. We repeated this process 100 times for each card. To automate this process we wrote a perl script to execute the *cardctl* command to turn the PCMCIA slot on (this denoted the insertion of the NIC) and off (this denoted the ejection of the NIC). To ensure synchronization with the traffic collection process, we used the Network Time Protocol (NTP) through a wired Ethernet connection and used the *crontab* command to schedule execution of our perl script periodically.

5.1.2 Data Collection

During the scanning process, the client broadcasted probe request frames on different channels. We used three 3GHz Pentium 4 Toshiba laptops with Linux Redhat 9 as sniffers to collect traffic on multiple channels independently. Each sniffer was configured with an internal Atheros wireless NIC and an external wireless NIC inserted through the PCMCIA slot. Three Linksys WPC11 cards were used as the external NICs, two of which came from the client setup. As a result, while observing the client using the Linksys cards, we were only able to collect traffic on 5 channels (1 through 5)

simultaneously. For the experiments with the Lucent and DLink cards we were able to collect traffic on 6 channels (1 through 6) simultaneously.

To be able to see the raw IEEE 802.11 frames on a particular channel, each card was put into monitor mode on an assigned channel using the *iwconfig* and *wlanctl-ng* utilities [41]. The sniffers used *tcpdump* [42] to collect the frames with timestamps into a traffic capture file. To automate the data collection process each sniffer used a perl script to execute the *tcpdump* command. To ensure that the capture covered the scanning period, *crontab* was used to schedule execution of the perl script on the sniffers at the same time as the execution of the perl script at the client. Synchronization was maintained with the client using the Network Time Protocol (NTP) through a wired Ethernet connection. The data collection process resulted in 100 traffic capture files for each channel per card (total of 2800 traffic capture files).

5.2 Statistical Analysis

Before applying spectral analysis, we conducted a statistical evaluation on the scanning traffic generated. For each card, an evaluation was done per channel. First we counted the number of probe request frames sent during each experimental trial for each channel per card. Figure 4 shows the results and Table 1 (page 36) summarizes these results. The results show that the lucent cards were much more aggressive in sending probes than the other cards. For all of the cards, channels 4 and 6 were probed more often than channels 1, 2, 3, and 5.

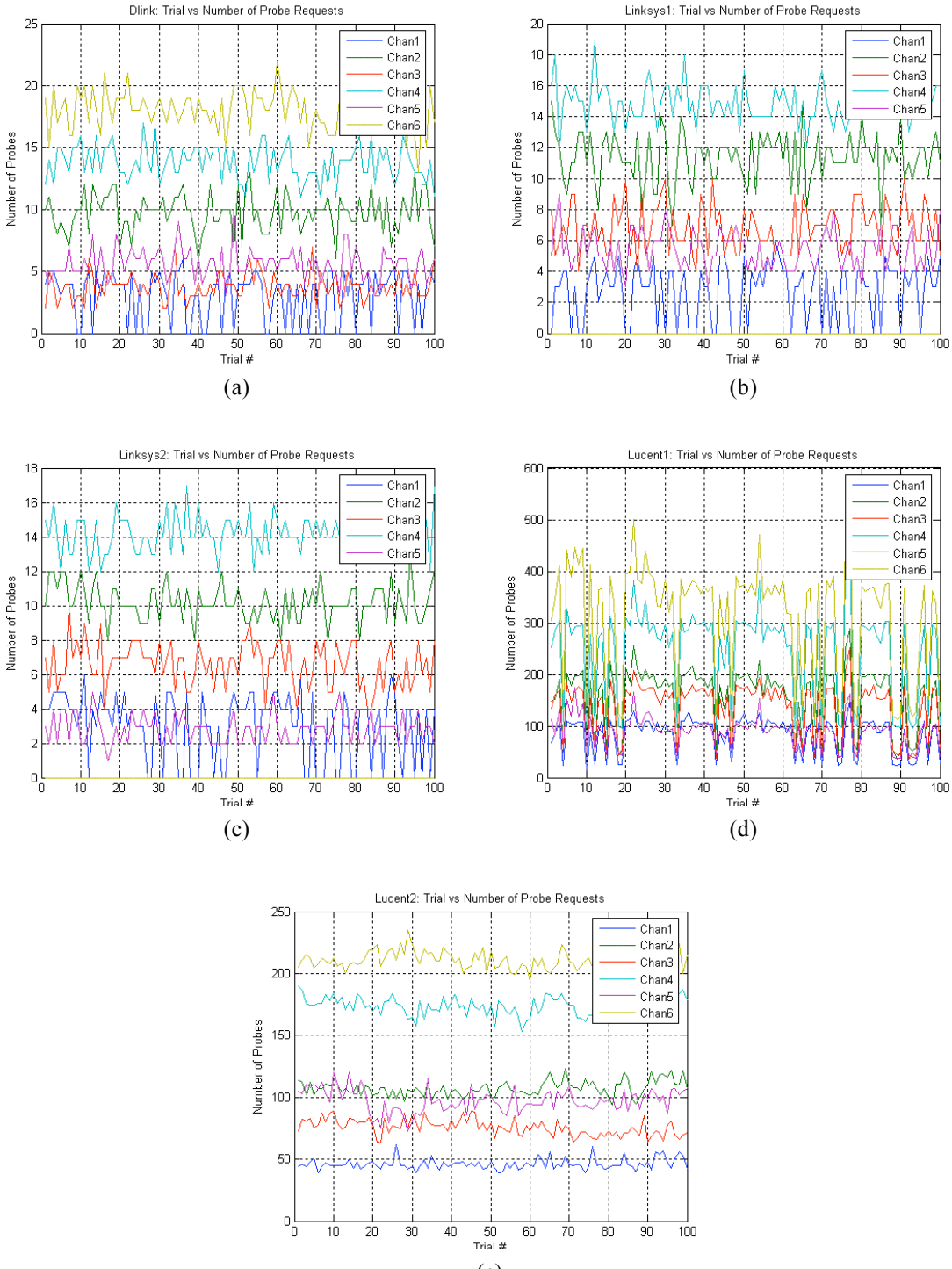
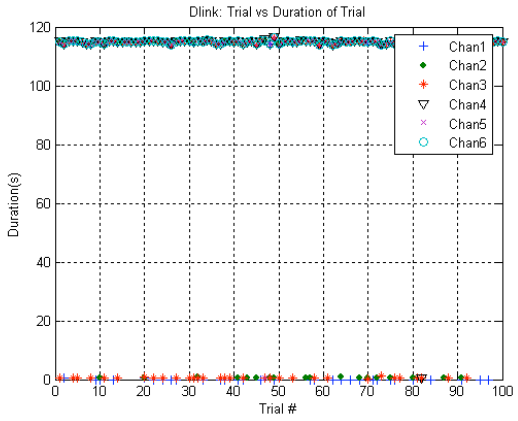


Figure 4 Number of probe request frames sent by each wireless NIC

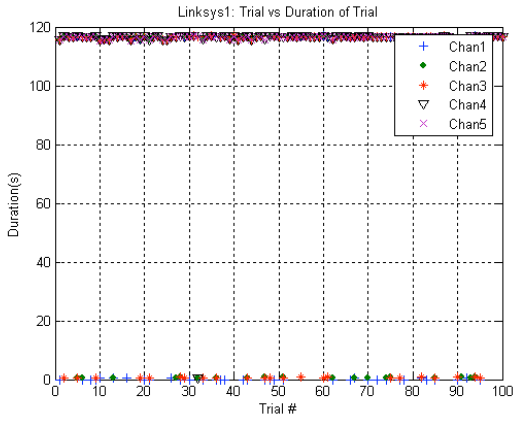
Table 1 Number of Probe Request Frames Transmitted

		Channel 1	Channel 2	Channel 3	Channel 4	Channel 5	Channel 6
Dlink	min	0	6	2	11	3	13
	max	6	13	7	17	10	22
	mean	3.02	9.7	3.77	13.79	5.6	18.12
	median	4	10	4	14	6	18
Linksys 1	min	0	7	4	12	3	
	max	6	15	10	19	9	
	mean	2.7	11.34	6.86	15.03	5.44	
	median	3	11	7	15	5	
Linksys 2	min	0	8	4	12	1	
	max	6	13	10	17	5	
	mean	2.98	10.23	6.63	14.29	2.85	
	median	4	10	7	14	3	
Lucent 1	min	15	37	36	93	36	113
	max	150	288	251	439	175	548
	mean	83.09	155.24	136.18	245.14	88.85	312.03
	median	103.5	181.5	158	284.5	94.5	360
Lucent 2	min	39	94	63	153	73	187
	max	62	123	89	191	120	235
	mean	46.1	107.29	75.66	174.4	97.25	209.56
	median	45	107	75	174	96.5	209

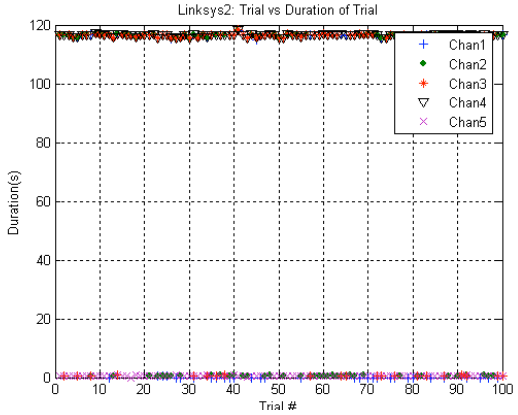
Next we measured the length of time each card probed a channel within the 4 minute observation period. The results are shown in Figure 5 and summarized in Table 2 (page 38). For most of the channels, the Lucent cards scanned the channel almost the entire 4 minutes. However, the Dlink and Linksys cards scanned most of the channels for about 2 minutes. We also examined the manner in which the cards probed a channel. We observed that for most channels, the Lucent cards would send a burst of probes, then wait a period of time (typically 2, 8, or 10 seconds) to transmit the next burst of probes (Figure 6a). The Dlink card sent a burst of probes and waited about 115 seconds to transmit one more probe request frame (Figure 6b). The Linksys cards behaved in the same manner as the Dlink card as shown in Figure 6c.



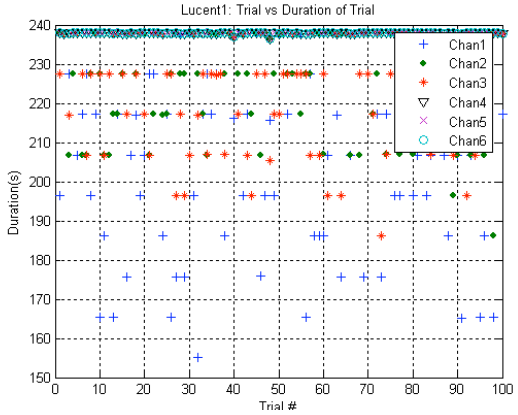
(a)



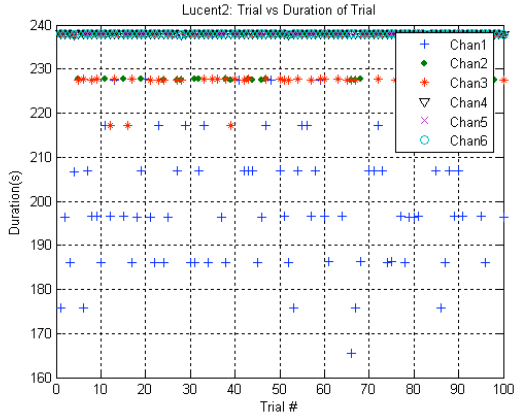
(b)



(c)



(d)

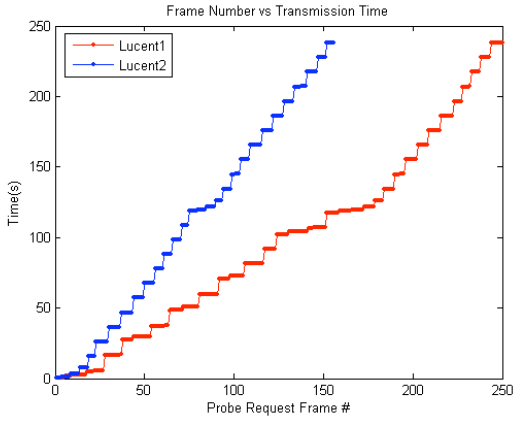


(e)

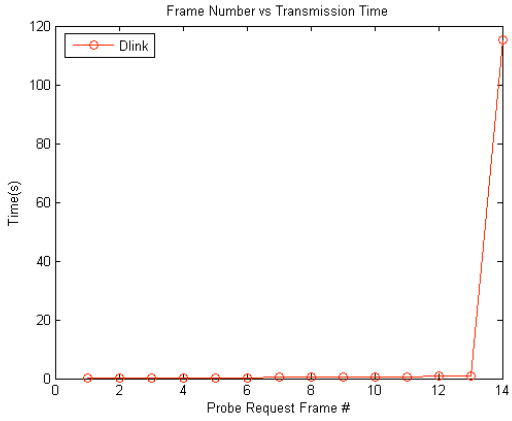
Figure 5 Duration of probing for each wireless NIC

Table 2 Duration of Probe (seconds)

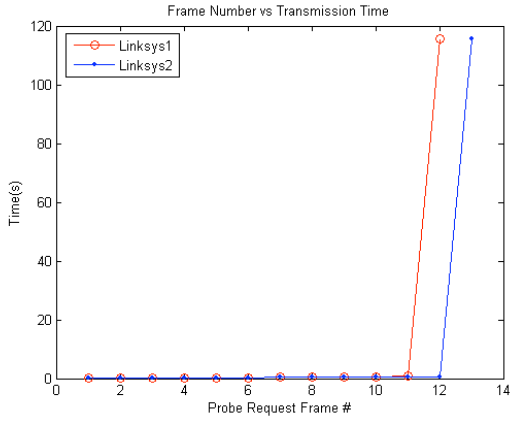
		Channel 1	Channel 2	Channel 3	Channel 4	Channel 5	Channel 6
Dlink	min	0	0.46614	0.34602	0.70156	0.5176	113.85
	max	115.36	115.44	116.45	116.6	116.4	116.47
	mean	75.80909	94.29148	78.29326	113.8627	113.6692	114.899
	median	114.705	114.94	114.805	115.125	114.92	115.02
Linksys 1	min	0	0.57264	0.4843	0.68081	115.37	
	max	116.93	116.91	116.91	117.08	116.93	
	mean	74.55683	94.44631	89.81147	115.4179	116.4071	
	median	116.395	116.57	116.51	116.74	116.58	
Linksys 2	min	0	0.50257	0.45159	115.58	0	
	max	118.13	118.21	118.28	118.33	0.79882	
	mean	78.00183	71.29663	92.14231	116.5573	0.53967	
	median	116.325	115.745	116.565	116.74	0.53106	
Lucent 1	min	155.04	186.1	186.12	236.52	236.51	236.52
	max	237.92	237.97	237.97	238	238.05	238.03
	mean	209.4641	226.6719	225.0143	237.8896	237.8829	237.8897
	median	217.075	227.57	227.55	237.92	237.91	237.92
Lucent 2	min	165.42	227.47	217.22	237.83	237.76	237.84
	max	238.02	238.09	238.05	238.1	238.09	238.11
	mean	206.8664	235.3699	232.9854	237.9971	237.9744	238.0009
	median	206.85	237.94	237.92	238	237.98	238



(a)



(b)



(c)

Figure 6 Example of burstiness in the scanning mechanism for each NIC

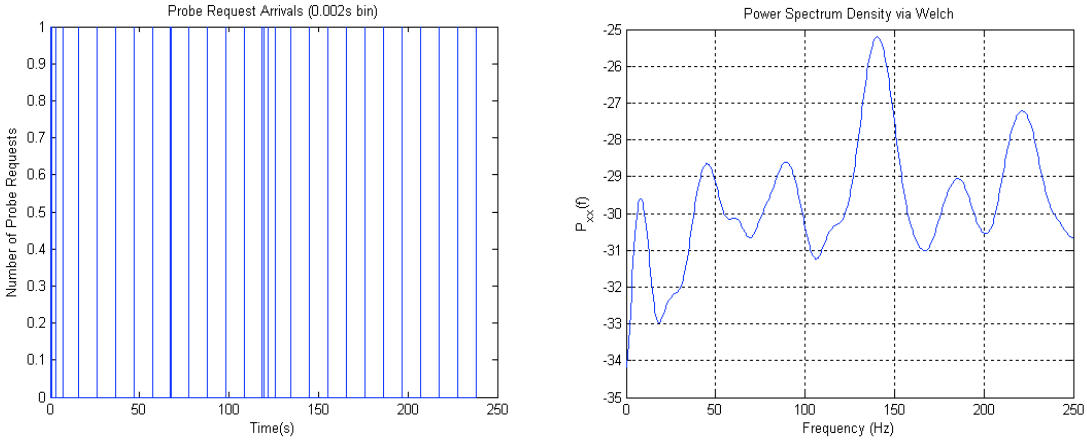
Table 3 Excerpt from capture file for Lucent2 card on channel 4

No.	Time	Source	Destination	Protocol	Info
1	0	Agere_49:96:d0	Broadcast	IEEE 802.11	Probe Request, SSID:Broadcast
2	0.028662	Agere_49:96:d0	Broadcast	IEEE 802.11	Probe Request, SSID:Broadcast
3	0.04302	Agere_49:96:d0	Broadcast	IEEE 802.11	Probe Request, SSID:Broadcast
4	0.064545	Agere_49:96:d0	Broadcast	IEEE 802.11	Probe Request, SSID:Broadcast
5	1.106644	Agere_49:96:d0	Broadcast	IEEE 802.11	Probe Request, SSID:Broadcast
6	1.114149	Agere_49:96:d0	Broadcast	IEEE 802.11	Probe Request, SSID:Broadcast
7	1.128559	Agere_49:96:d0	Broadcast	IEEE 802.11	Probe Request, SSID:Broadcast
8	1.135679	Agere_49:96:d0	Broadcast	IEEE 802.11	Probe Request, SSID:Broadcast
9	1.150033	Agere_49:96:d0	Broadcast	IEEE 802.11	Probe Request, SSID:Broadcast
10	3.238618	Agere_49:96:d0	Broadcast	IEEE 802.11	Probe Request, SSID:Broadcast
11	3.260586	Agere_49:96:d0	Broadcast	IEEE 802.11	Probe Request, SSID:Broadcast
12	3.28206	Agere_49:96:d0	Broadcast	IEEE 802.11	Probe Request, SSID:Broadcast
13	3.289228	Agere_49:96:d0	Broadcast	IEEE 802.11	Probe Request, SSID:Broadcast
14	3.303583	Agere_49:96:d0	Broadcast	IEEE 802.11	Probe Request, SSID:Broadcast
15	7.420728	Agere_49:96:d0	Broadcast	IEEE 802.11	Probe Request, SSID:Broadcast
16	7.428233	Agere_49:96:d0	Broadcast	IEEE 802.11	Probe Request, SSID:Broadcast
17	7.442589	Agere_49:96:d0	Broadcast	IEEE 802.11	Probe Request, SSID:Broadcast
18	7.44976	Agere_49:96:d0	Broadcast	IEEE 802.11	Probe Request, SSID:Broadcast
19	7.485649	Agere_49:96:d0	Broadcast	IEEE 802.11	Probe Request, SSID:Broadcast

5.3 Spectral Analysis

We processed the traffic collected in the capture files using the signal processing technique discussed in Chapter 4. Table 3 is an excerpt of a capture file from one of the trials with the Lucent2 client card on channel 4. In our experiments we generated 100 capture files for each channel per card. We processed each capture file in the following manner. The probe request frames and associated time stamps were extracted from the traffic capture file to represent the time series of events. Next we sampled the time series at a rate of 500 Hz, counting the number of probe request frames that arrive in each 0.002 second bin. Figure 7a illustrates a uniformly sampled signal representation of the traffic capture file from the Lucent2 card on channel 4 in Table 3. Next we applied the Welch method to estimate the power spectral density. We used a 1024-point FFT, a segment length of 64 data points, an overlap of segments by 32 data points, and the Hanning window to configure the Welch method. With a sampling rate of 0.002 seconds, we

were able to observe periodicity in the scanning process over a range of 250 Hz. Figure 7b is the PSD for the input signal encoded in Figure 7a. Processing the capture files in this manner generated 100 PSDs for each channel per card. Appendix A contains a subset of the output graphs. To keep the graphs legible, we avoid plotting every PSD and only selected a few PSDs to plot per graph.



(a) (b)

Figure 7 Uniformly sampled signal of the arrival rate of probe request frames for Lucent2 on channel 4 (a) and corresponding PSD estimate (b)

5.3.1 Qualitative Results

The peaks in the PSD estimates show periodicity in the scanning process on all channels for all cards. The frequency points at which the peaks occur corresponds to the transmission rates of the probe request frames. The magnitude of the peaks is proportional to how often the transmission rate occurs. General observations can be made by visually comparing the PSD graphs (Appendix A) for different channels and different cards. Below we discuss our observations.

Dlink

- The PSD estimates for repeated trials on the same channel are similar.
- The choice in the sampling rate resulted in the occurrence of harmonics.
- The fundamental frequency for scanning on channel 1 is 20 Hz.
- Channels 3 and 5 exhibit the same behavior as channel 1.
- The fundamental frequencies for scanning on channel 2 are 20Hz, 40Hz, and 60Hz. The prominent peak at 60Hz contains significantly more power, indicating that probes are sent at this rate much more regularly than the other frequencies.
- Channels 4 and 6 exhibit the same behavior as channel 2.

Linksys

- The PSD estimates for repeated trials on the same channel are similar.
- The PSD estimates are similar between both of the Linksys cards on all channels.
- The PSD estimates are similar to Dlink for channels 1, 2, 4, and 5 (see observations listed for Dlink card).
- The fundamental frequencies for scanning on channel 3 are 20Hz, 40Hz, and 60Hz. However, magnitude of difference at these frequency points is small. In some trials, the PSD for channel 3 is similar to channel 1.

Lucent

- The PSD estimates for repeated trials on the same channel are similar.
- The PSD estimates between both of the Lucent cards are similar for channels 4, 5, and 6.
- The PSD estimates for channels 4, 5, and 6 have the most prominent peaks around 135 Hz and 215 Hz.

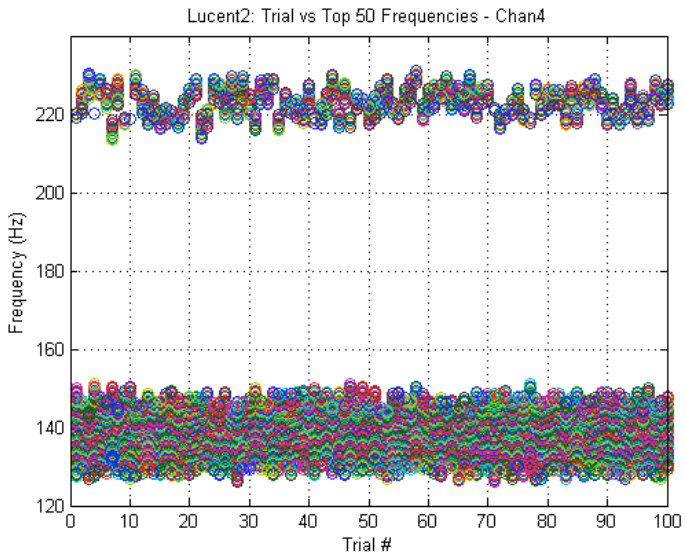


Figure 8 Plot of the top 50 frequencies for all trials on Lucent2 channel 4

5.3.2 Quantitative Results

The previous section examined the PSD estimates visually, which allowed comparison of the complete spectra. To numerically compare spectra we used the approach discussed in Chapter 4, which uses a subset of the PSD values. For our analysis of the scanning process we elected to use 50 frequency points from the PSD that exhibited the greatest amount of power. These key frequency points represent the most prevalent sending rates of the probe request frames. For each trial, we let the set of frequencies $F = \{f_1, f_2, f_3, \ldots f_{50}\}$ with the greatest amount of power constitute the spectral profile that we use to compare spectra. Figure 8 plots the set F for each trial on Lucent2 channel 4 (see Appendix B for the remaining plots of the other cards and channels). The formation of a horizontal line at a particular frequency range is indicative of the similarity in the spectral content among trials on the same channel. For example, Figure 8 shows that the spectral profile for all trials on channel 4 of Lucent2 contain frequencies between 130-150Hz and 218-225Hz. Conversely, if the data points are spurious, then the spectral

content among the trials on the same channel are different at those frequencies. Even though we are only working with a subset of the values given by the PSD, the results plotted in these graphs reiterate the observations made above in the qualitative results section. For each channel we arbitrarily selected 1 out of the 100 trials to use as the representative trial $T_{\mathbf{R}}$ and its corresponding profile to be the representative spectral profile $F_{\mathbf{R}} = \{f_1, f_2, f_3, \ldots f_{50}\}$ for that channel. The tables in Appendix C illustrate the frequency values that make up the spectral profile $F_{\mathbf{R}}$ for the representative trial on each channel. Next we compared the spectral profile of the remaining trials to $F_{\mathbf{R}}$ to measure robustness of $F_{\mathbf{R}}$. The results of the comparisons on channel 4 are shown in Table 4-Table 8 (the remainder of the results are shown in Appendix D). The first column of the table groups the contiguous frequencies of $F_{\mathbf{R}}$ into frequency ranges. The second column tells what portion of $F_{\mathbf{R}}$ is within a particular range. The last column is the percent of trials with a spectral profile that contain frequencies in the same range as the frequencies as $F_{\mathbf{R}}$. The last row is the most important and indicates the percent of trials with a spectral profile containing frequencies within all the ranges associated with $F_{\mathbf{R}}$. (For this analysis, trials that sent less than 3 probe request frames were excluded. This primarily affects channel 1 and channel 3 of the Dlink card and channel 1 for the Linksys cards.) Our results showed that the comparison of spectral profiles matched best on channels 4 and 6, where 90% or more of the trials matched the spectral profile $F_{\mathbf{R}}$ of the representative trial. However, since experiments were not done on channel 6 for the Linksys cards, due to hardware limitation, we continued our analysis solely on channel 4.

Table 4 Dlink Channel 4

Frequency Range (Hz)	Percent of F_R	Percent Match
55.176 - 64.453	40%	100%
115.72 – 123.54	34%	100%

176.27 – 182.13	26%	90%
All		90%

Table 5 Linksys1 Channel 4

Frequency Range (Hz)	Percent of F_R	Percent Match
55.664 - 64.941	40%	100%
116.7 - 124.51	34%	100%
177.73 - 183.59	26%	97%
All		97%

Table 6 Linksy2 Channel 4

Frequency Range (Hz)	Percent of F_R	Percent Match
55.176 - 64.453	40%	100%
115.23 - 123.54	36%	100%
176.76 - 182.13	24%	94%
All		94%

Table 7 Lucent1 Channel 4

Frequency Range (Hz)	Percent of F_R	Percent Match
126.46 – 146	82%	100%
221.19 - 225.1	18%	90%
All		90%

Table 8 Lucent2 Channel 4

Frequency Range (Hz)	Percent of F_R	Percent Match
131.84 - 149.41	74%	100%
218.75 - 224.61	26%	94%
All		94%

Next we used the spectral profile $F_{\mathbf{R}}$ generated for channel 4 to compare NICs. Figure 9 plots the frequency values of the spectral profile of channel 4 for each NIC. Cards of the same type had a similar spectral profile. Additionally, the Dlink card had a similar profile to the Linksys cards. This can be attributed to the fact that Dlink and the Linksys cards used the same *prism2_cs* driver software. For Dlink and both of the Linksys cards, the concentration of $F_{\mathbf{R}}$ is between 55 and 65 Hz (frequency ranges 116-

125Hz and 176-184 are harmonics). This indicates that the transmission rate of probe request frames is most often sent around 0.0167 seconds. The F_R for both of the Lucent cards indicate that most of the power is concentrated between 126-149Hz and between 210-225Hz. This corresponds to a transmission rate between .0076 and .0079 seconds and a second transmission rate between .0044 and .0048 seconds.

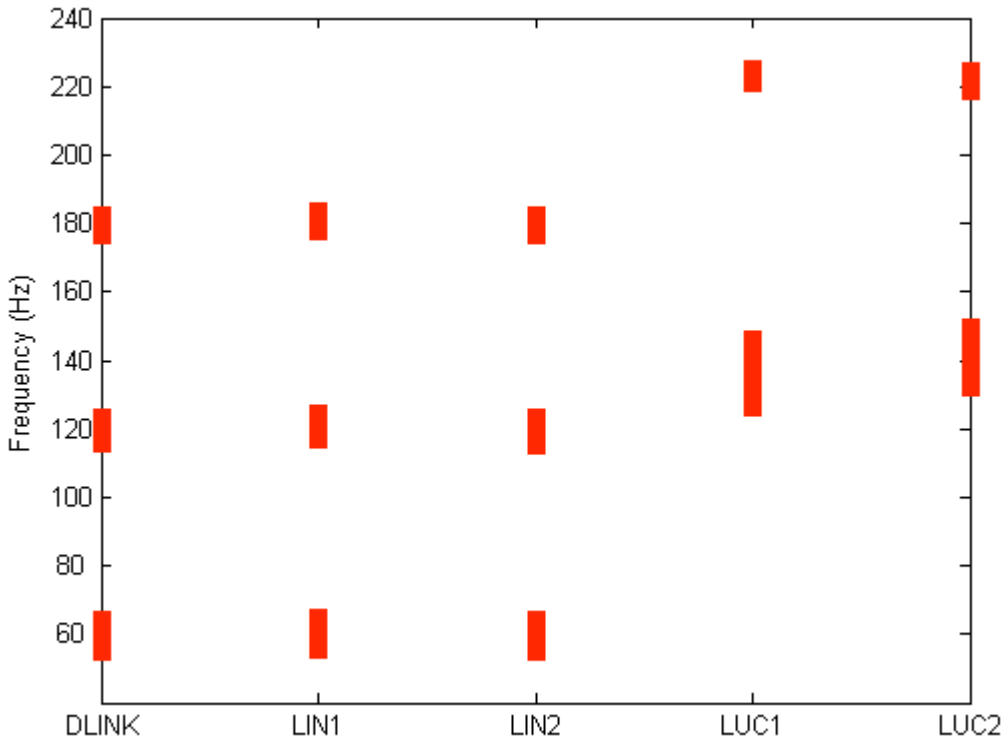


Figure 9 Plot of spectral profile F_R for channel 4 of each card.

5.4 Summary

The scanning mechanism implemented in the NIC is a viable attribute to identify cards. Spectral analysis proved to be a stable approach for analyzing the scanning process as evidenced by the ability to reproduce the PSD for repeated trials. Ideally one would like to listen on all channels at once to monitor the scanning process of a client to develop a scanning profile. However, sniffing on all channels is impractical.

Additionally, profiling on certain channels was shown to be better than others, as scanning algorithms tend to favor some channels over others, because vendors try to anticipate the channels most likely to offer network connectivity to minimize the amount of time the card spends scanning. Out of the subset of channels we examined, our results showed that monitoring channel 4 is the best channel for profiling wireless NICs. Results showed that there was more regularity and stability in the way the scanning mechanism of all card types probed channel 4 (and channel 6 for Lucent and Dlink). This is also evident by the fact that there were significantly more probes on channels 4 and 6 than channels 1, 2, 3, and 5. As a result, there was more communication traffic to observe and a better opportunity for identifying card types. Once we compared the spectral profile of all the cards for channel 4 we showed that different cards manufactured by the same vendor and used the same driver had the same spectral profile. We were also able to discern between Lucent and Linksys/Dlink. Linksys and Dlink had identical spectral profiles, likely because they used the same software driver. This led us to conclude that the scanning mechanism is implemented in the software driver of the NIC. The scanning mechanism of the Lucent cards was more aggressive than the other cards. The Lucent cards transmitted more probes, sent probes at a faster rate, and probed channels for a longer period of time.

6 NIC IDENTIFICATION USING RATE SWITCHING

We have pinpointed rate switching as another IEEE 802.11 function that can be used to identify NICs (section 3.1.2). A rate switching algorithm dynamically adapts the transmission rate, per packet, based on the channel conditions to optimize performance. Additionally, the implementation of the rate switching algorithm dictates the number of frames to transmit at the selected rate, how often to change rates, and the order in which the transmission rate is selected. This directly impacts the periodicity of a wireless stream. We use signal processing to extract the spectral content imposed by the rate switching algorithm to identify wireless network interface cards. We begin this chapter with an empirical analysis to show that rate switching is a naturally occurring phenomenon. Next we discuss the impact of rate switching on the periodicity of wireless traffic in our controlled experiments. Finally, we identify NICs using rate switching in a real environment.

6.1 Empirical Analysis of Rate Switching

Unlike scanning, which automatically starts when the card is powered up, rate switching is invoked based on the perceived condition of the link. Therefore, we conducted an empirical analysis to characterize the rate switching phenomenon. We demonstrate, with measurements taken at a wireless hotspot, that rate-switching occurs with reasonably high frequency and is also more likely to happen the longer a NIC has been transmitting.

6.1.1 Experimental Setup

Analysis was conducted at a local hotspot on the campus of Georgia Institute of Technology. Over the course of 7 days we captured all traffic on the wireless network. We used a Toshiba laptop with a Linksys WPC11 wireless card to collect traffic. We put the wireless card into monitor mode using the *wlanctl-ng* utility and stored the captured traffic using *tcpdump*. With the card in monitor mode we were able to detect the transmission rate associated with each packet collected, while *tcpdump* appended a timestamp to each packet. We used the timing information and transmission rate to generate statistics. Traffic was collected for a total of 13.3 hours over the course of 7 days. During our observation period, there were a total of 61 wireless clients that visited the hotspot.

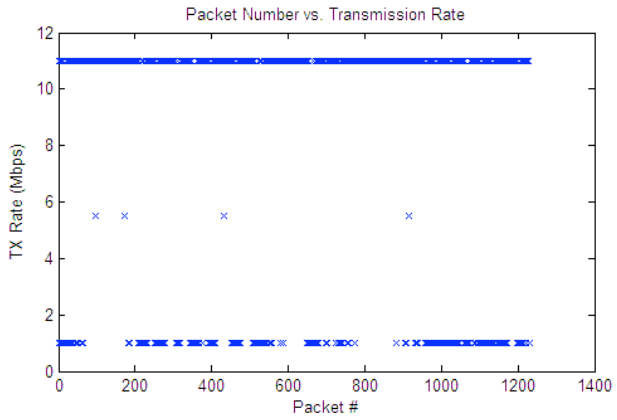


Figure 10 Host at local hotspot invoking rate switching

6.1.2 Results

The results of our analysis show that rate switching is common at the hotspot. While this is definitely true for the hotspot we monitored, it is likely that RF interference occurs at most hotspots. Therefore, rate switching is likely a widespread, common phenomenon. Figure 10 shows the transmission rate of each data frame transmitted by

one of the clients at the local hotspot. This particular client had undergone 279 changes to its transmission rate. Overall, Figure 11 shows how often rate switching occurred for all wireless clients over the entire observation period. Figure 12 shows that 67% of the clients performed rate switching, while 33% did not switch rates. Out of the clients that did not perform rate switching, 85% sent less than 9 packets (Figure 13). If we exclude the non-switching clients that sent less than 9 packets (assuming that these clients were never properly authenticated to the network), the percent of clients that perform rate switching becomes 92% (Figure 14).

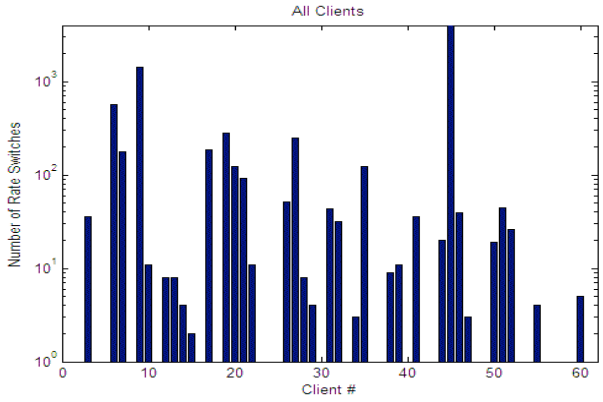


Figure 11 Number of rate switches for each client

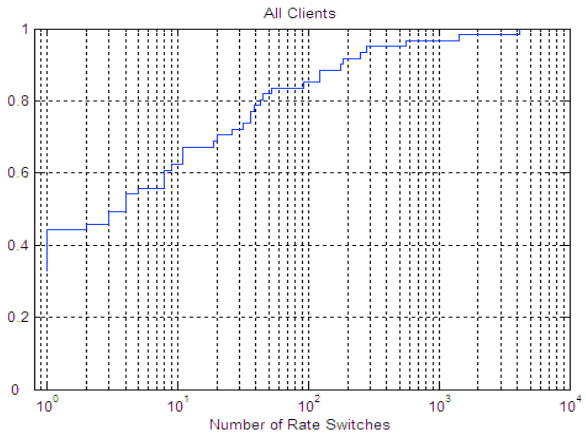


Figure 12 CDF of the number of rate switches for all clients

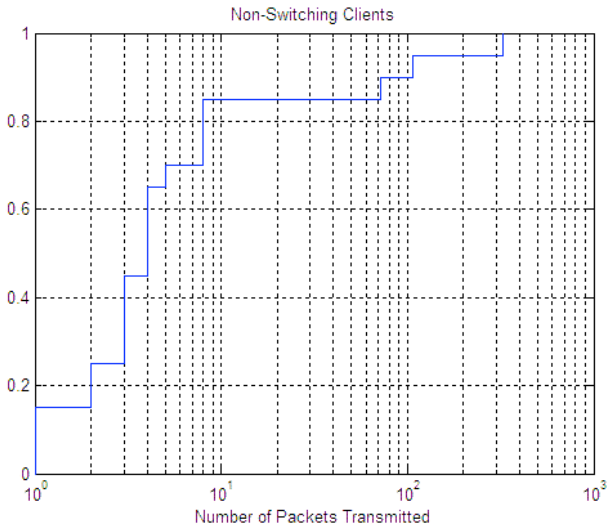


Figure 13 CDF of the number of packets transmitted by clients that did not perform rate switching

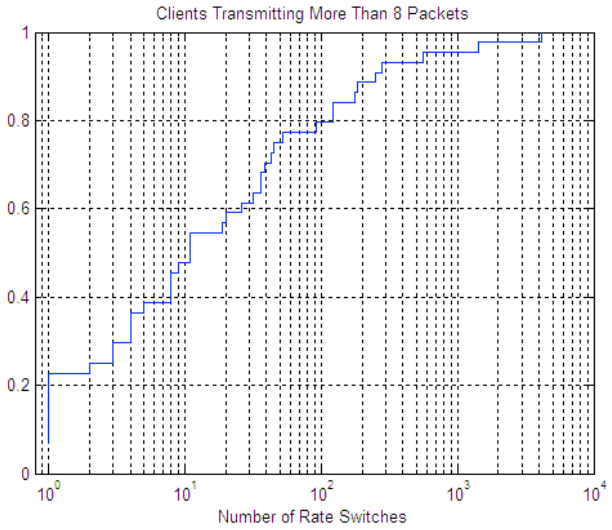


Figure 14 CDF of the number of rate switches excluding non-switching clients that transmitted less than 9 packets

Examining only the wireless clients that applied rate switching, Figure 15 shows that 90% transmitted more than 37 packets and 88% were connected to hotspot more than 2 minutes. Also, 85% of these clients switched rates within the first 3 minutes of their connection.

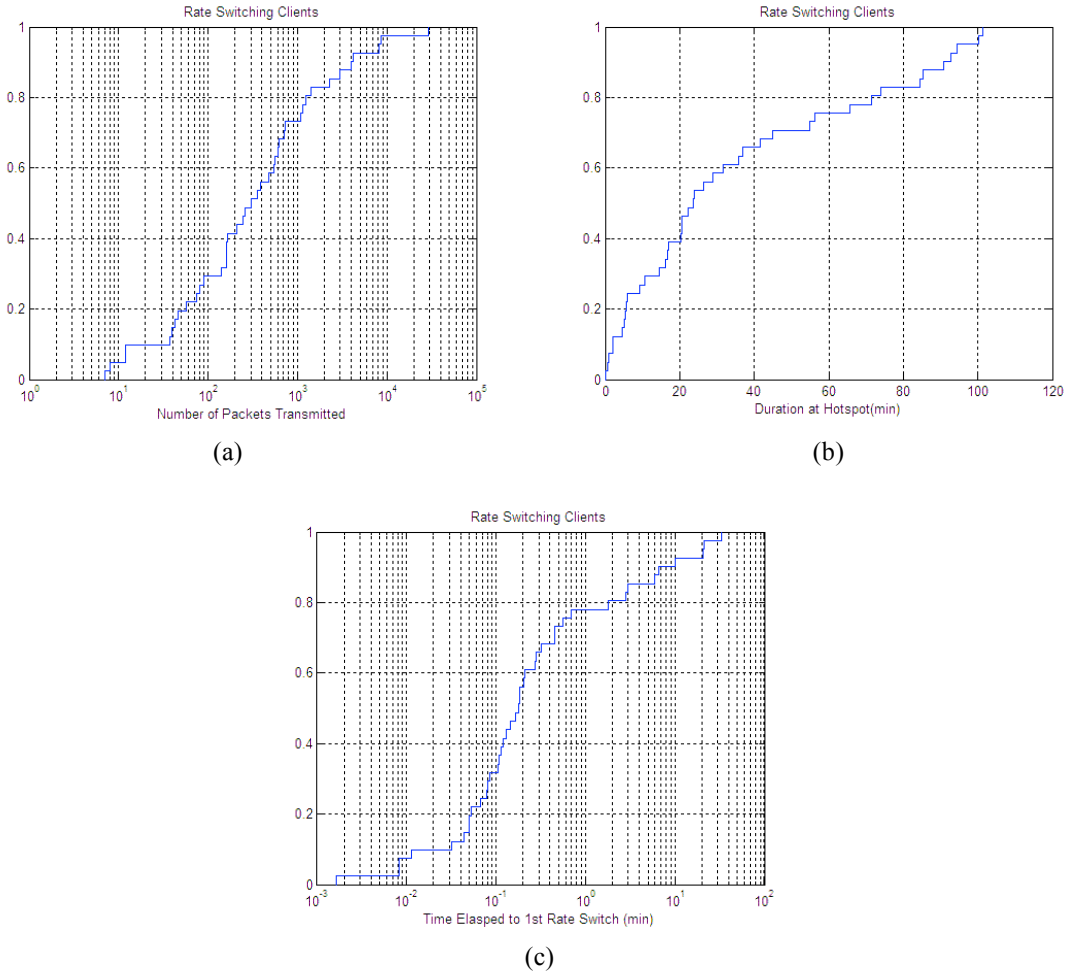


Figure 15 Rate switching clients – (a) CDF of number of packets transmitted, (b) CDF of duration at hotspot, (c) CDF of time elapsed at 1st rate switch

6.1.3 Conclusion

We conclude that rate switching is a phenomenon that occurs. Our results show that the longer a wireless client is connected to the network and the more packets it transmits, the more likely rate switching is to occur. Therefore, rate switching is a viable attribute within the wireless NIC for distinguishing between cards.

6.2 Controlled Experiments

Through controlled experiments we show that rate switching influences data transmission patterns in a manner that is observable through spectral analysis. We

examine the differences in the spectral characteristics of a card when it has undergone rate switching versus when the card does no rate switching. We also compare differences in spectral content caused by rate switching algorithms of different card types.

6.2.1 Client Setup

We used a 1GHz Toshiba laptop as the wireless client. The client had two PCMCIA slots to interface with wireless cards. On the first interface we tested three NICs: D-Link DWL-650, Linksys WPC11, and Lucent/Orinoco Gold. During the experiments the Lucent card used the *orinoco_cs* software driver. The Dlink and Linksys cards used the *prism2_cs* software driver. We had the client to generate a traffic load of 2.4Mbps. The load was light enough to not stress the host, but heavy enough to cause the NIC to be the bottleneck in the wireless system so that it is the primary factor influencing the behavior of the traffic. We used the *sock* [43] program to establish a user datagram protocol (UDP) connection carrying constant bit rate (CBR) traffic generating a 1470-byte packet every 5 milliseconds. For each card, the laptop sends data over the wireless link through a wireless router to a desktop, which connects via a wired connection.

6.2.2 Data Collection

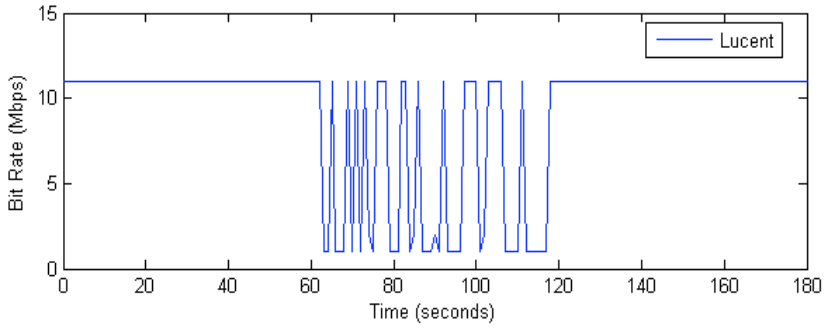
The client was also responsible for collecting traffic. Using its second interface, an additional card was inserted and set to monitor mode to capture traffic. The client also executed a perl script to periodically (on a 1 second interval) record the transmission rate of the card sending data given by the status information available through the *iwconfig* utility.

6.2.3 Wireless Environment

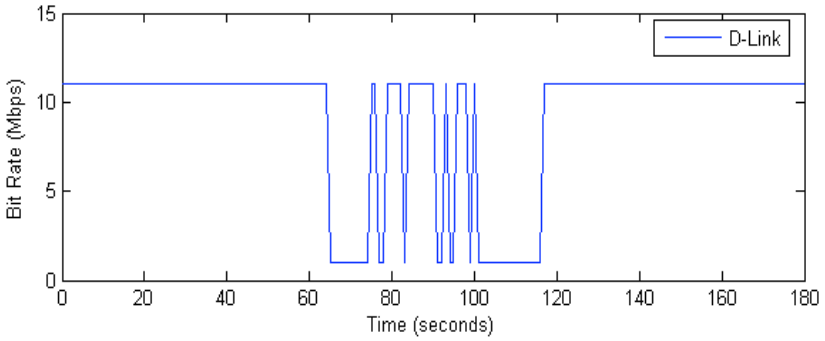
In a real environment, rate switching occurs due to changes in channel conditions caused by noise. This noise may be caused by network contention, interference from neighboring networks operating on the same channel, mobility of a wireless client, non-802.11 devices operating in the same frequency range, etc. During this experimental evaluation, we wanted to control the invoking of the rate switching algorithm. To do so, we used the microwave as an artificial noise source to alter the condition of the wireless link. A microwave is capable of causing interference with the radio waves of an 802.11 network because it operates in the 2.4 GHz band. Since the energy of the microwave is normally shielded from the outside, a small 6 inch covered wire was inserted in the door with a portion of the wire hanging on the outside. In our experiments we started streaming data for 60 seconds, and then turned on the microwave causing an instant pulse of noise. After 60 seconds, the microwave was turned off and data continued streaming for another 60 seconds. We were able to trigger rate switching as seen in Figure 16.

6.2.4 Spectral Analysis

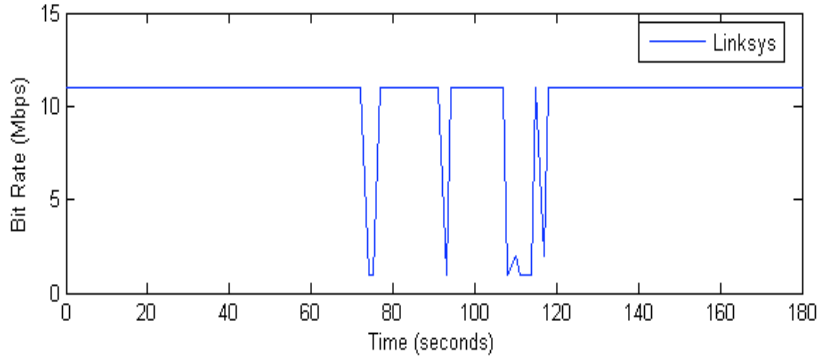
We analyzed the captures using the encoding process and PSD estimation as discussed in Chapter 4. We partitioned the analysis into three 60 second parts: the interval before injecting noise, the interval with noise, and the interval after injecting noise. For each partition, we used a sampling bin of 2 ms, which represents a frequency range up to 250 Hz. We also wanted to maintain the highest possible frequency resolution in the PSD estimate to reveal any distinctive peaks that may be at close frequencies. To do so, we set the segment size to the length of the signal and set the number of FFT points to the next power of two greater than the length of the signal. With these



(a)



(b)



(c)

Figure 16 Cards invoking rate switching

parameters, the Welch method did not perform any averaging or smoothing to the peak energies, capturing all of the spectral detail embedded in the signal.

Spectral analysis of the traffic trace prior to injecting noise generated a similar PSD for all three card types as illustrated by Figure 17. The PSD also reveals that power is concentrated at discrete frequency points. Each card has the most prominent peaks at

100Hz and 200Hz (this indicates that data frames were most frequently sent at 10 ms and 5ms intervals). Similarities in the PSDs confirmed that the NICs behaved the same in transmitting data frames when there was no rate switching (i.e., when the condition of the link is perceived as good).

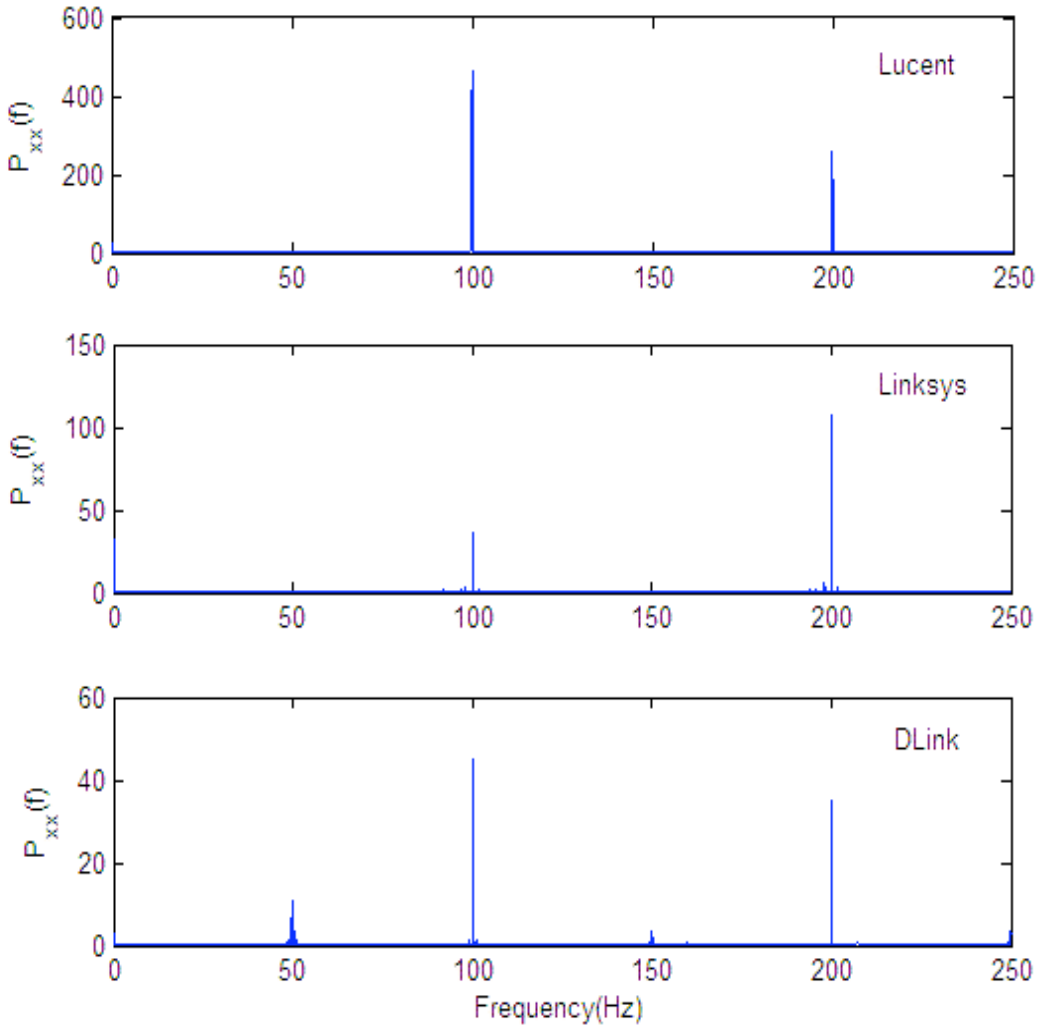


Figure 17 PSD prior to injecting noise when there was no rate switching

During the interval in which noise was injected into the wireless environment, each card generated a distinctive PSD as shown in Figure 18-Figure 20 (pages 57 and

58). In contrast to the noiseless period, we also observed that prominent peaks are no longer at discrete points, but scattered throughout the frequency range. For example, in Figure 18 the Lucent NIC still has prominent peaks at 100Hz and 200Hz (that were seen before injecting noise), but new distinctive peaks are found at the lower frequencies (0-10Hz and 50-60Hz). The spread of prominent peaks throughout the frequency range indicates that a host is transmitting data frames at different rates. This type of behavior is expected while a NIC is executing its rate switching algorithm.

Once we generated the spectrum, we used the normalized cumulative spectrum (NCS) to compare spectral characteristics between the NICs. The normalized cumulative spectrum *C(f)* is the amount of power *p(f)* in the range 0 to *f* normalized by the total power. The amount of power *p(f)* is given as

$$p(f) = \sum_{i=0}^{f-1} \frac{(\hat{P}_{xx}(i) + \hat{P}_{xx}(i+1))}{2}$$

and the normalized cumulative spectrum *C(f)* is given as

$$C(f) = \frac{p(f)}{p(f_{\max})} .$$

We plotted the results of the NCS along with the PSD in Figure 18Figure 20. The slope of the NCS of the Linksys NIC (Figure 19) is almost linear with a modest variation in the slope over the range of 90Hz to 130Hz (and 190-210Hz), indicating that the power spreads (somewhat evenly) across this frequency range. DLink (Figure 20) shows a concentration of power around 50Hz indicated by the strong rising slope in the NCS at that frequency point. The strong rising slope of the NCS for Lucent (Figure 18) indicates a concentration of power around 10Hz (and 100 Hz).

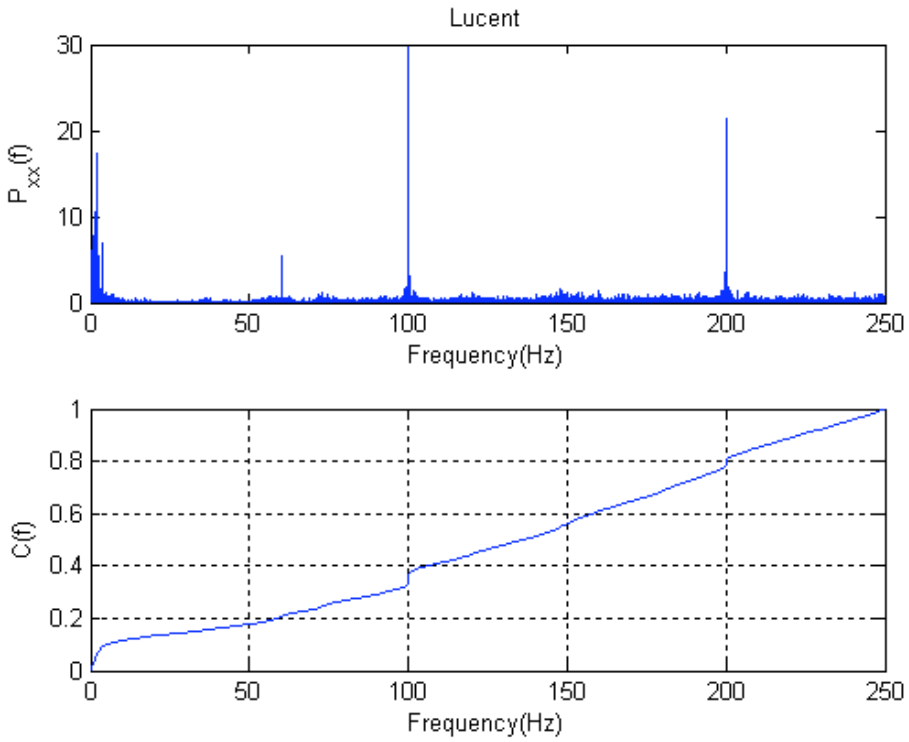


Figure 18 PSD (top) and cumulative PSD (bottom) of Lucent card during rate switching

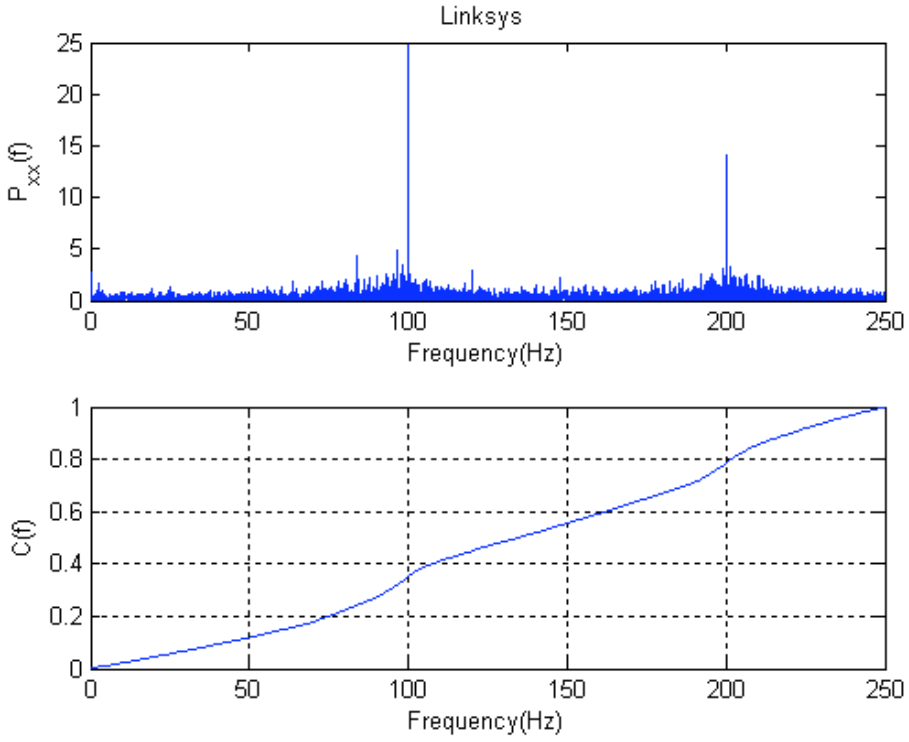


Figure 19 PSD (top) and cumulative PSD (bottom) of Linksys card during rate switching

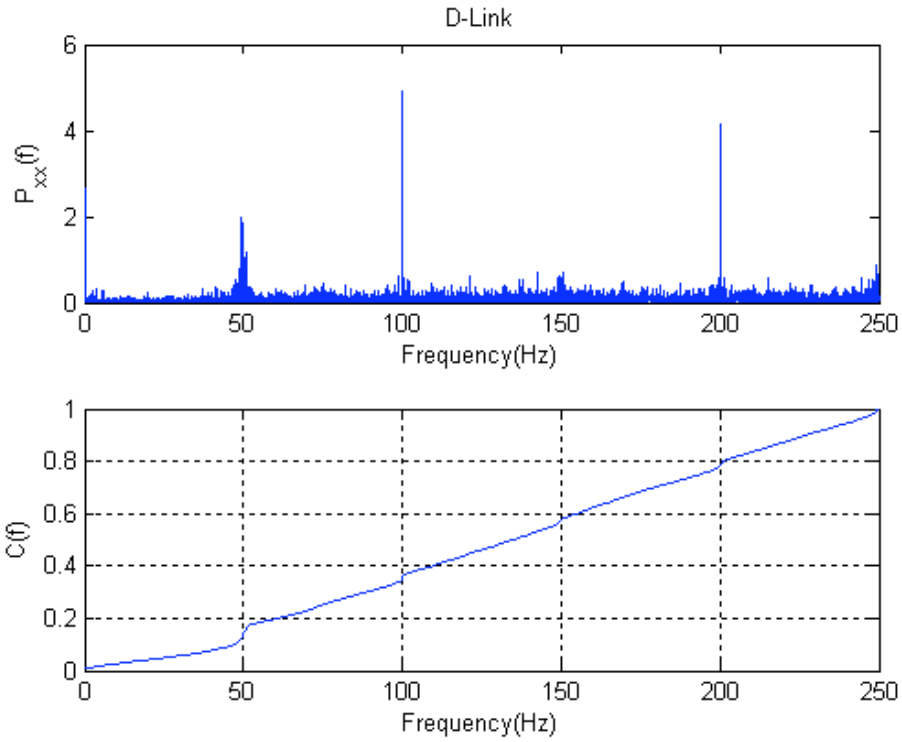


Figure 20 PSD (top) and cumulative PSD (bottom) of DLink card during rate switching

To numerically compare the spectra between NICs, we locate the frequency points that exhibit the greatest amount of power. These key frequency points estimate the most prevalent sending rates of the NIC during rate switching. For our evaluation, we chose the top 50 frequency points to constitute a frequency set, $F = \{f_1, f_2, \ldots f_{50}\}$, as the spectral profile of a NIC. Table 9 displays the distribution of the set F for each NIC. By examining the range where the majority (54% or more) of the set F is located, we can distinguish between NICs. A Lucent NIC can be identified by 54% of its top frequencies concentrated between 0-10Hz. This indicates that a Lucent NIC most often sends data frames at a rate of 100ms during rate switching. The concentration of F for the Linksys card is over a broader range: 56% between 80-130Hz. A Linksys NIC most often

attempts to send data frames between 7.7ms and 12.5ms during rate switching. Whereas, the DLink NIC most often sends data frames between 17ms and 25ms indicated by a concentration of 54% of the set F between 40-60Hz. The selection of 50 frequency points as a spectral profile proved to be adequate, because the distribution of the set *F* coincides with the observations made using the NCS.

Table 9 Distribution of 50 Dominant Frequencies

Frequency Range	Lucent	D-Link	Linksys
0-10	54%	8%	2%
40-50	-	28%	-
50-60	4%	26%	-
80-90	-	-	10%
90-100	12%	8%	34%
100-110	10%	4%	8%
120-130	-	-	4%
140-150	-	2%	2%
150-160	-	6%	-
190-200	20%	4%	16%
200-210	-	12%	24%
220-230	-	-	-
230-240	-	2%	-

6.2.5 Conclusion

Using rate switching to help identify NICs is feasible, because rate switching does affect the periodicity of a wireless stream. For each card, we showed that the spectrum for traffic during rate switching was different from the spectrum on traffic without rate switching. We also showed that cards manufactured by different vendors had markedly different spectral profiles during rate switching, which suggest that each of these cards implemented a different rate switching algorithm.

6.3 Real-World Experiments

We have shown that wireless clients frequently exercise rate switching and that it is feasible to extract differentiating spectral characteristics as a result of rate switching for

the identification of a NIC. In this section we conduct experiments to show that rate switching is a stable attribute for identifying NICs in a real environment. Unlike the controlled environment, this environment will consist of multiple heterogeneous clients contending for the network, multiple access points connected to the Internet, clients entering and leaving the network, and various user applications traversing the network. In addition to comparing cards by different manufacturers, we evaluate the differences and similarities within the same manufacturer. We also examine the affects of different higher-layer protocols on the spectral profile for rate switching.

6.3.1 Experimental Setup

The following experiments were conducted at a hotspot on the campus of Georgia Institute of Technology. Our wireless client was a 1GHz Toshiba laptop with Redhat 9.0 that transmitted data to a remote node connected to the Internet (Figure 21). We extended on the controlled experiments to include 2 additional Linksys WPC11 cards and an additional Lucent Orinoco/Gold card for a total of 6 NICs. (The cards identified in this section as Linksys3, Lucent1, and Dlink were the same cards used during the controlled experiments.) The Dlink and Linksys cards used the *prism2_cs* driver software; and the Lucent cards used the *orinoco_cs* driver software. For each card we generated three separate traffic flows: one UDP flow and two TCP flows. The UDP traffic was generated using the *sock* program to transmit a 1470-byte packet every 5 milliseconds. Each UDP flow lasted approximately 10 minutes. To generate the TCP traffic the client used FTP to upload a 164 Mbyte file to the remote node. The FTP sessions lasted 9 to 14 minutes.[1]

[1] During the experiments with the Linksys3 card, the card would often change wireless channels during the FTP session. As a result, the traffic captures were 1 to 2 minutes longs.

A second laptop, placed next to the client, was used to collect traffic at the hotspot. We collected traffic in the same manner as the other experiments using *tcpdump*. However, for these experiments we used a newer version of the *wlanctl-ng* utility which allowed the sniffer to prepend a *prism* header to the 802.11 frame while collecting traffic. The *prism* header allowed us to know the transmission rate and other physical layer information for every packet.

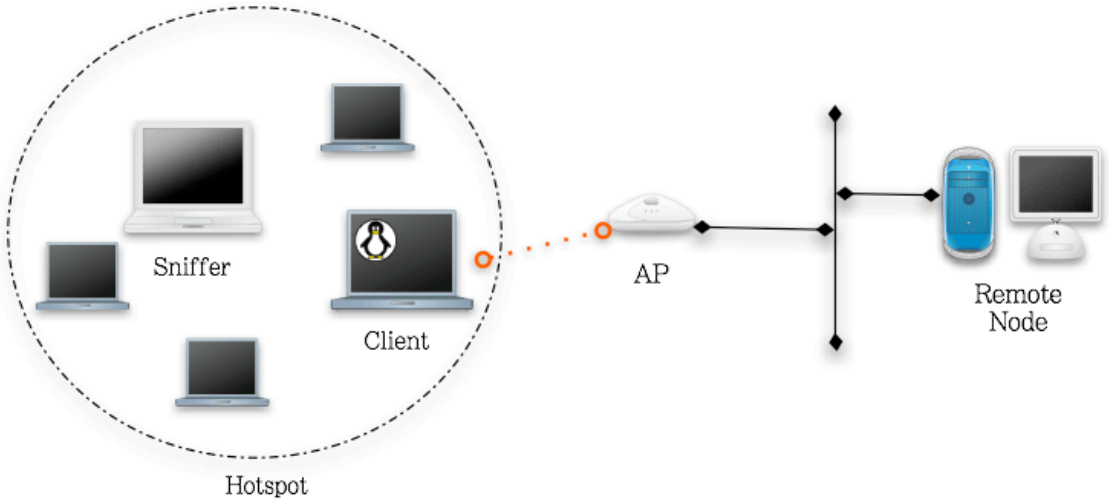
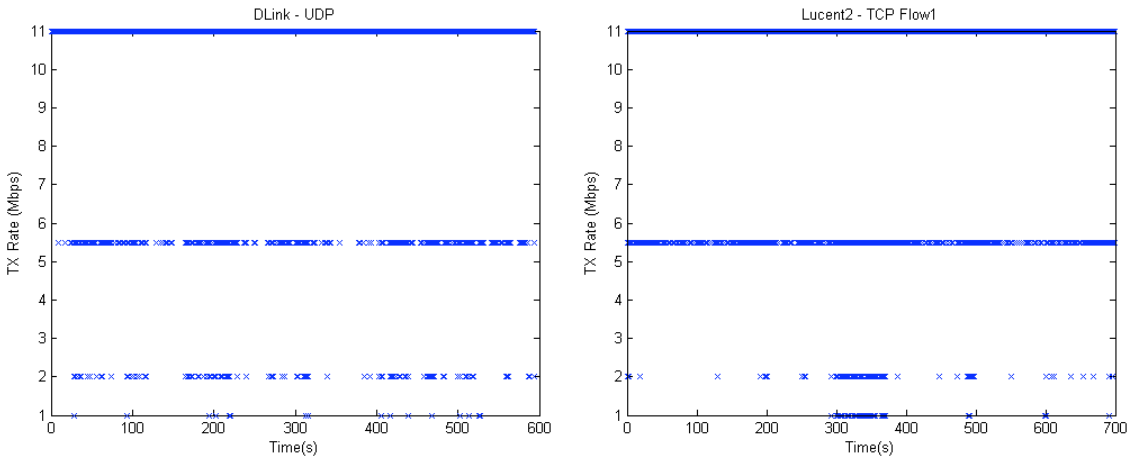


Figure 21 Experimental Setup

6.3.2 Analysis

For each experiment we extracted the transmission rate and time stamps associated with data frames sent by our client to the access point. We used the transmission rate information to calculate the number of rate changes that occurred during each session. We found that all cards exercised rate switching while streaming traffic for all flows. Figure 22 shows the DLink wireless network interface cards invoking rate switching during a UDP session and a Lucent card invoking rate switching during a TCP session. Similar graphs can be seen for all cards and other traffic flows in Appendix E.



(a) (b)

Figure 22 NICs at hotspot invoking rate switching during UDP session

To create the time series of events, we used the data frames and corresponding timestamps. The time series was sampled at a rate of 600Hz, counting the number of data frames sent in each .0167 second bin. The sampled signal representing each flow was partitioned into 60 second segments. Then we estimated the PSD for each segment of the flow independently. To calculate the PSD we used a 1024-point FFT, we sectioned the signal using 1024 data points with 50% overlap between sections, and used the Hanning windowing function. Figure 23 plots the PSD results for the first three segments of the TCP-flow1 for the Lucent1 NIC. Similar graphs can be found for all experiments in Appendix F. Across all cards and flow types, visually comparing the spectra among different segments within the same traffic flow revealed similarities. This indicates that the impact rate switching has on traffic throughout the succession of the flow is steady.

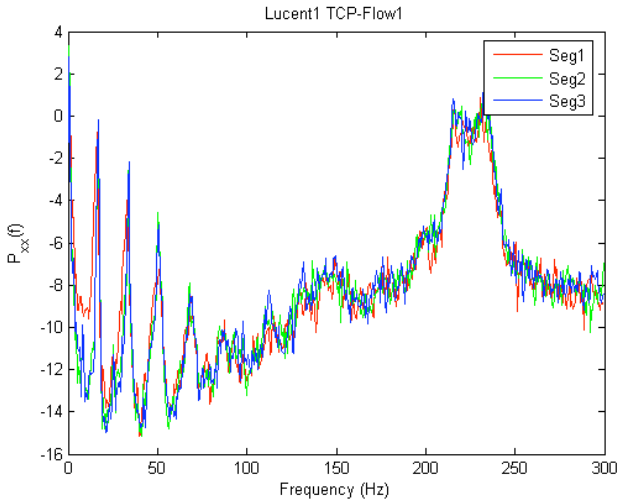


Figure 23 PSD of TCP-Flow1 for the Lucent1 card

To quantitatively compare spectra between segments of traffic within the same flow, we obtained the top 50 frequencies for each 60 second segment to represent the spectral profile $F_{seg} = \{f_1, f_2, f_3, \ldots f_{50}\}$ using the approach outlined in section 4.4. Figure 24 illustrates the top 50 frequencies for the Lucent1 TCP-flow1 (Appendix G contains similar graphs for the other cards). While only using a fraction of the values from the PSD estimate, the formation of a straight line near 0Hz, 8 Hz, 16Hz, and across the range of 212-239 Hz preserves the fact that spectral content for different segments is similar.,

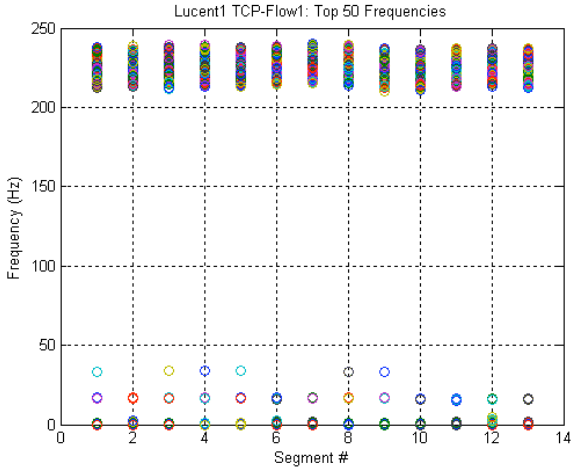


Figure 24 Plot of the top 50 frequency points that constitute the spectral profile for each segment of the Lucent1 TCP-Flow1

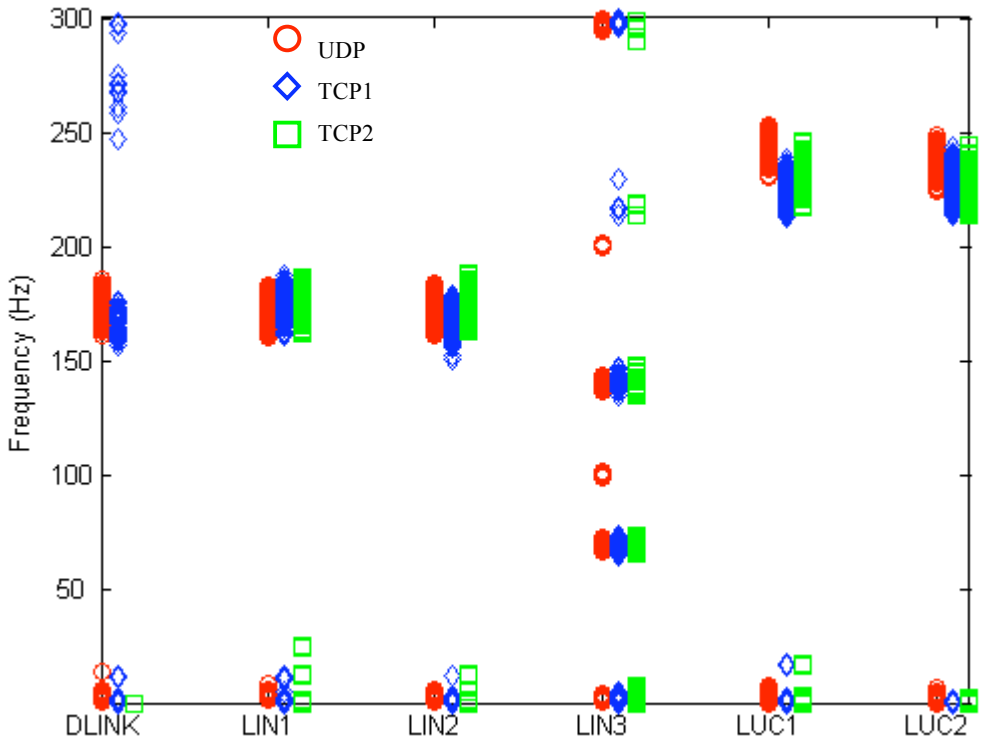


Figure 25 Plot of the spectral profile F_R for each NIC and traffic type.

Next we selected the spectral profile of one segment from each flow to be the representative spectral profile F_R for the entire flow. Figure 25 plots F_R for each traffic type per card. The exact values of F_R can be viewed in Appendix H. Once we selected the representative profile, we measured how well the spectral profile of the other segments of the flow matched F_R Table 10 summarizes the results.

Table 10 Percent of Segments Matching F_R

	UDP	TCP1	TCP2
Dlink	87.5	90	-
Linksys1	83.3	100	100
Linksys2	100	100	100
Linksys3	75	n/a[2]	n/a[2]
Lucent1	100	100	100
Lucent2	100	100	100

[2] The length of the traffic captures was too short to have enough segments for an accurate comparison.

To finish our analysis we compare spectral profiles F_R between different flows and different cards. Reviewing the individual PSD plots in Appendix F and spectral profiles in Figure 25 we draw the following conclusions:

- For each card the spectral profiles for the TCP flows overlap with the spectral profile for the UDP flow. This indicates that the spectral profile for rate switching is not sensitive to the type of traffic. Reviewing the complete spectra shows there are some differences in the PSD between the different traffic types, but this occurs at frequency points where the magnitude of power is not as great as the power at the frequencies that they have in common.
- For the Lucent card set, both of the cards (Lucent1 and Lucent2) had a similar spectral profile indicating that both of these cards implement the same rate switching algorithm.
- Within the Linksys card set, Linksys3 had a different spectral profile from the other two cards even though they all used the same software driver. We speculate that Linksys3 is a different version, which may have different hardware and/or firmware from the other two Linksys cards. This suggests that the manufactures of the Linksys cards implemented the rate switching algorithm within the hardware and/or firmware of the NIC, rather than the driver software.
- The Dlink card behaved similarly to Linksys1 and Linksys2. Some versions of the DLink 650 card are based on the Intersil Prism chipset, which is the same chipset family used in Linksys cards. Dlink, Linksys1 and Linksys2 may all have had the same hardware. This would explain the similarities and coincide with the

speculation we made above that the rate switching algorithm for these types of cards is implemented in the hardware rather than the driver software.

Based on the observations we made above we can classify the six NICs into three classes as shown in Table 11. Class I has a concentration of power primarily between 160-180 Hz. This indicates that data frames were most frequently sent between 5.56 ms and 6.25 ms intervals during rate switching. The Class II card had a concentration of power around 70Hz and 100Hz (140Hz, 200Hz, and 300 are considered as harmonics). Accordingly, Class II sent data frames at 10ms and 14ms intervals during rate switching. The cards in Class III primarily operate between 213-249Hz, which corresponds to data frames being sent every 4.0 - 4.7ms during rate switching.

Table 11 Classification of wireless cards

Class I	Class II	Class III
Dlink	Linksys3	Lucent1
Linksys1		Lucent2
Linksys2		

6.3.3 Conclusion

Rate switching proved to be a stable attribute for identifying NICs. The distinctions we made in the controlled experiments upheld in the real environment. Additionally, we were able to make a distinction between cards manufactured by the same vendor. We also showed that rate switching behaved similarly for UDP and TCP traffic. Finally, we identified three classes of NICs based on the spectral characteristics of there rate switching algorithm.

7 CONCLUSION AND FUTURE WORK

7.1 Conclusion

The implementation of the IEEE 802.11 standard is organized into the hardware and software of a wireless card. We focused on differences in the implementation of the active scanning mechanism and rate switching algorithm, two functions required by the 802.11standard, for establishing the identity of wireless NICs. While scanning is a phenomenon that automatically occurs when the card is powered on, we showed that rate switching also occurs frequently. We used signal processing to analyze the periodicity embedded in the wireless traffic caused by active scanning and rate switching. We developed a technique to create a spectral profile from the periodic components of the traffic to use as the identity of a wireless NIC. Using the spectral profile generated from the scanning mechanism we were able to discern between cards that used different driver software. With the spectral profile of the rate switching algorithm, we were able to identify cards from different manufactures and within the same manufacturer independent of the driver software.

7.2 Future Work

As we extend our work it will be important to continue to explore the stability of the spectral profile. We have already considered different traffic types. It would also be useful to determine the impact of the composition of the host on the spectral profile. During our experiments we used a single host. Differences in the composition of a host such as CPU speed, type of operating system, and host load may affect the spectral

profile. If the spectral profile is sensitive to the composition of the host, we can restrict the classification of wireless system even further than just the type of NIC.

We also plan to investigate other attributes, such as the setting of the user configurable parameters (i.e., RTS threshold, maximum retries, etc.), from which we can extract a spectral profile. To do so we will need to consider other signal representations for wireless traffic. The current work primarily focuses on the arrival rate of probe request frames and data frames. We plan to examine other properties of a wireless frame to encode as a signal. For example, when investigating the impact of the setting of the RTS threshold, we could encode the arrival rate or inter-packet delay of retransmitted frames. Additionally, we could weight the encoding process using the size of the retransmitted frame as well.

The current approach for deriving a spectral profile worked well for capturing the important features of scanning and rate switching. However, there may be other spectral features that are distinctive but are unnoticed in the current approach because it would be overshadowed by other features that exhibited a higher magnitude of power. An alternative may be to group adjacent frequencies as one feature. Another alternative may be to establish thresholds relative to the total power. A more robust technique for comparing profiles would be need as the database of spectral profiles grows.

APPENDIX A: SCANNING POWER SPRECTRAL DENSITY PLOTS

This appendix contains excerpt of plots illustrating the PSD of the communication traffic generated from scanning mechanism of the NICs. Each graph plots the PSD of three arbitrary trials on each channel monitored for each NIC.

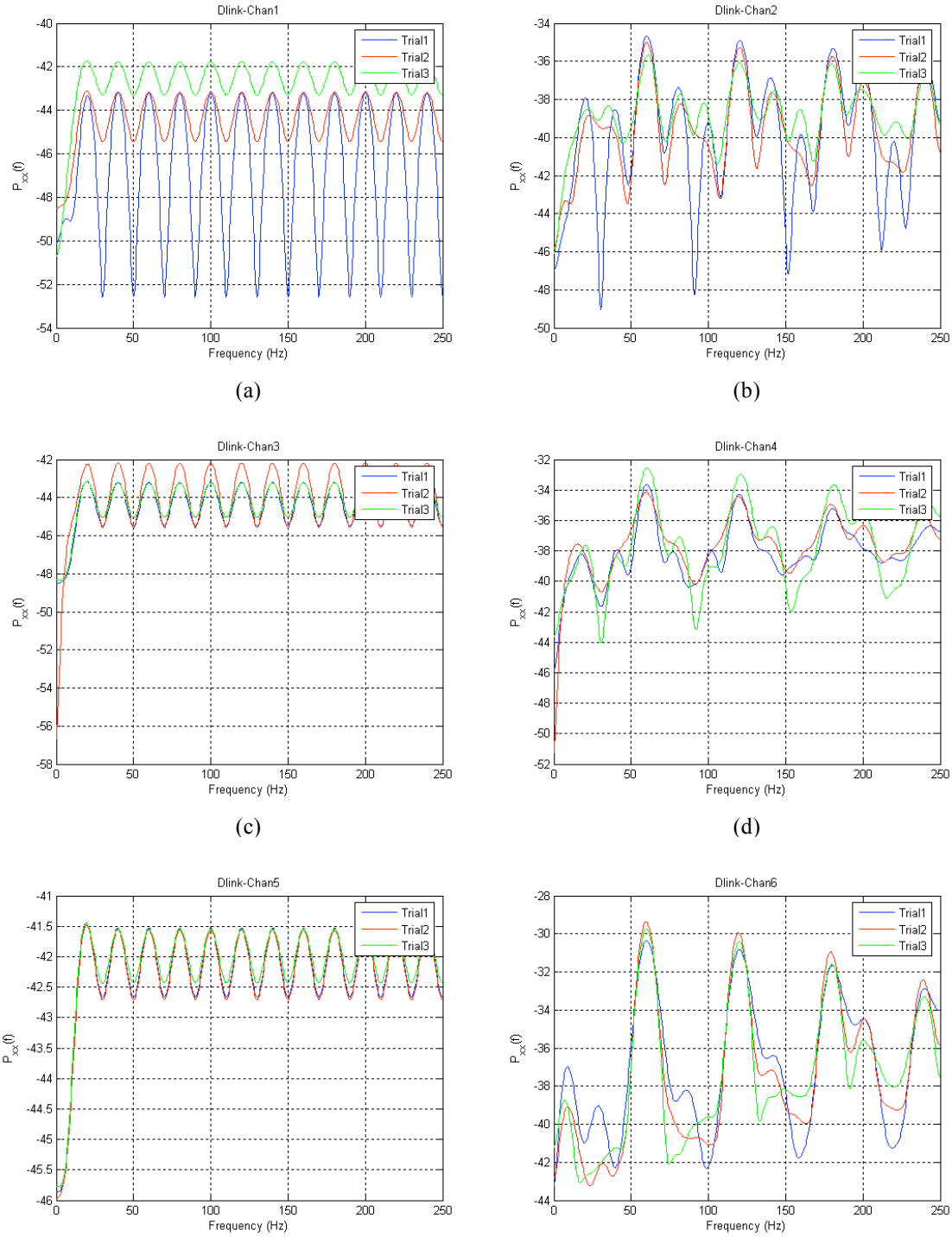


Figure 26 PSDs of Dlink card for channels 1 through 6

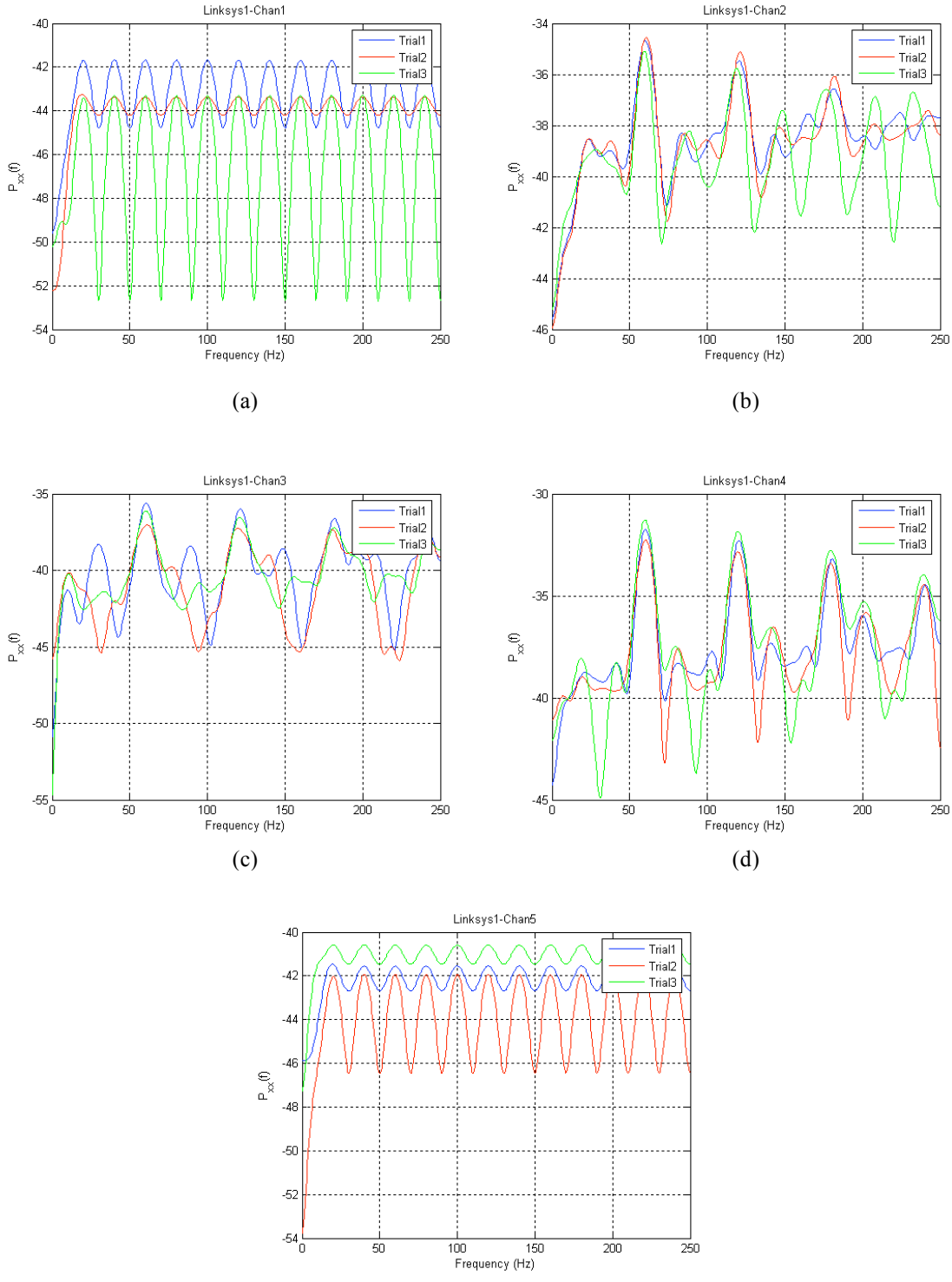
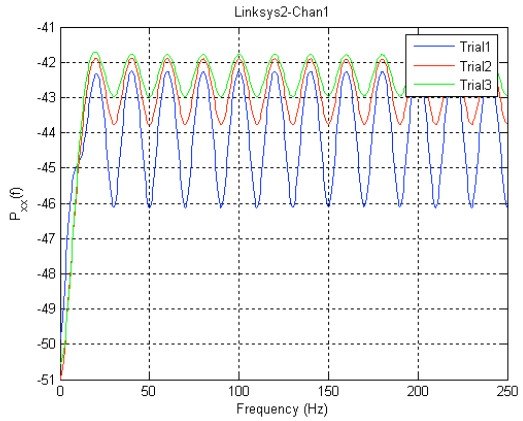
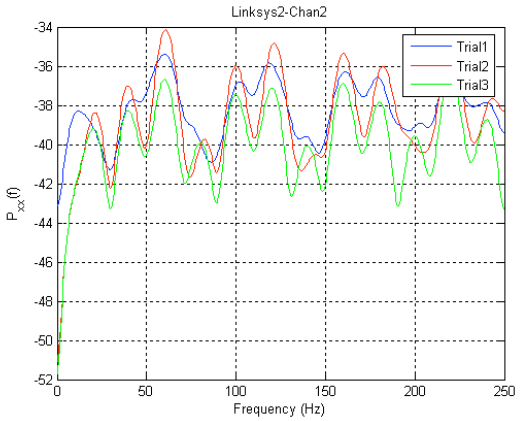


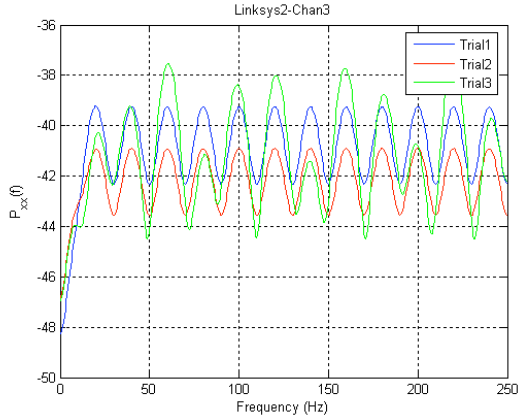
Figure 27 PSDs of Linksys1 card for channels 1 through 5



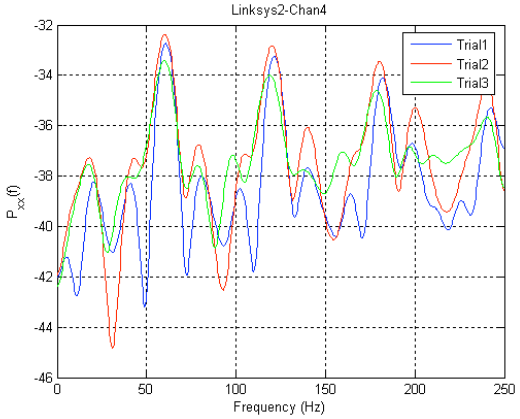
(a)



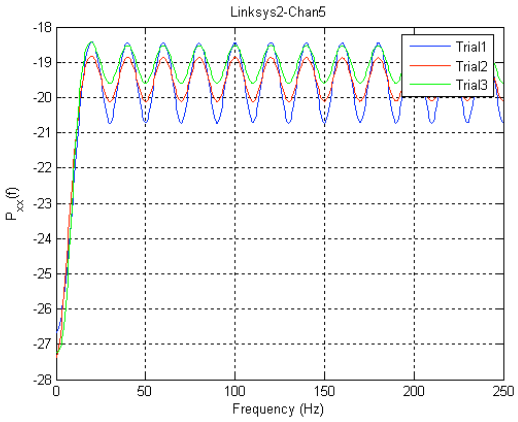
(b)



(c)



(d)



(e)

Figure 28 PSDs of Linksys2 card for channels 1 through 5

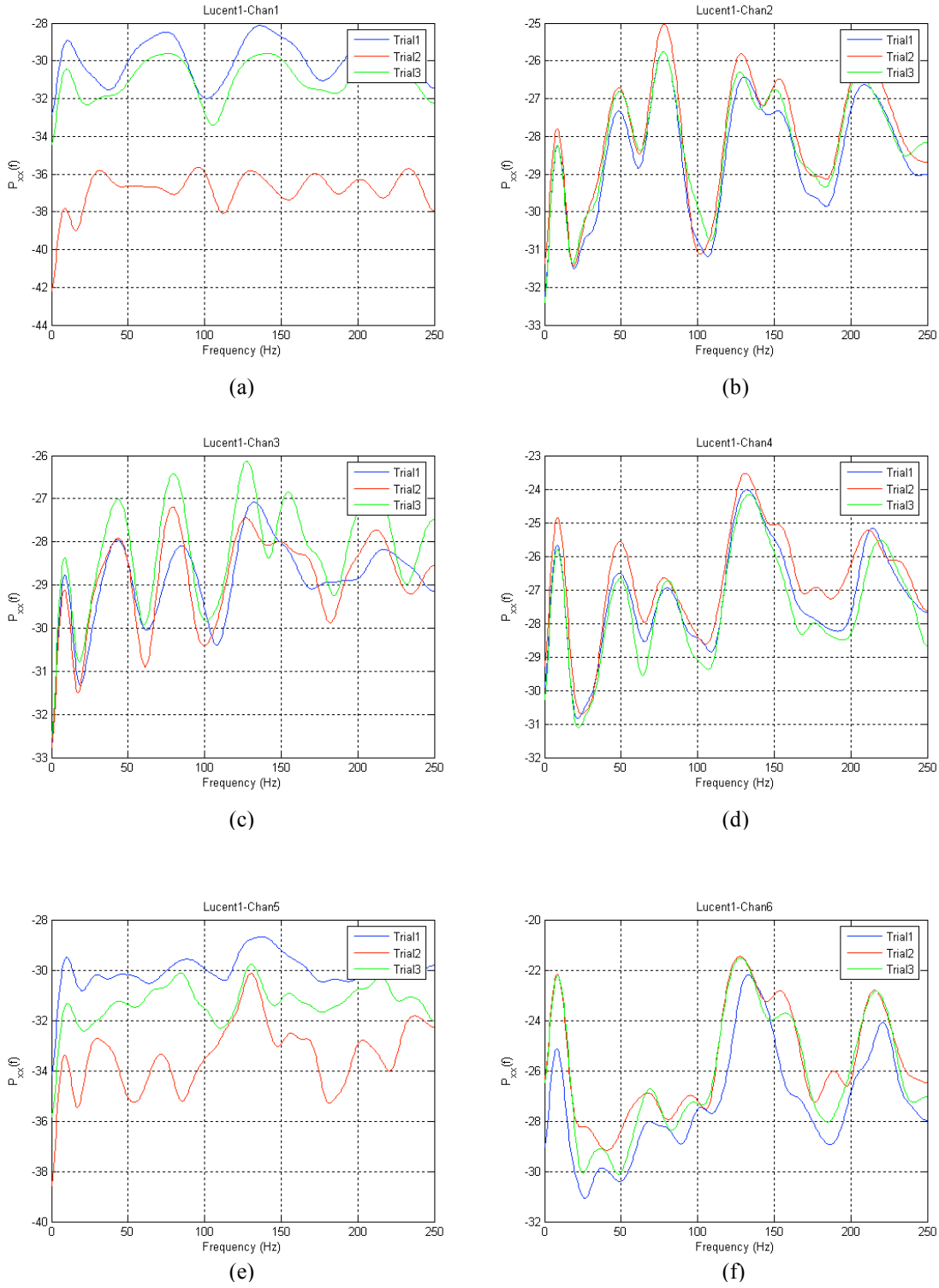
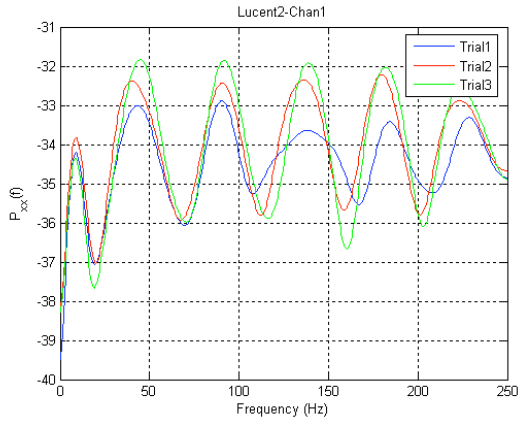
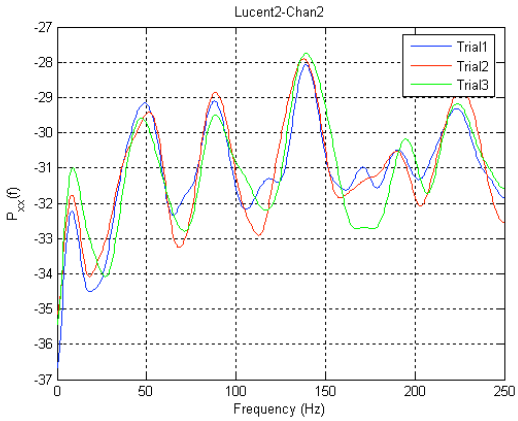


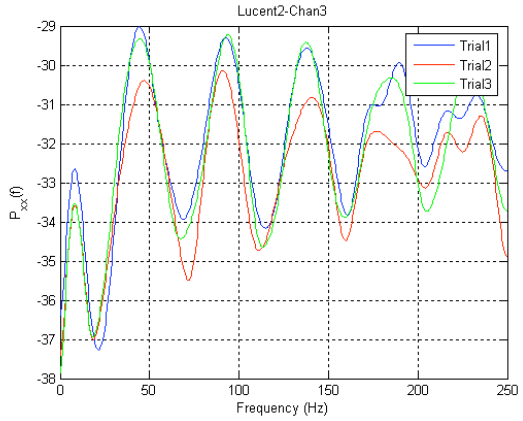
Figure 29 PSDs of Lucent1 card for channels 1 through 6



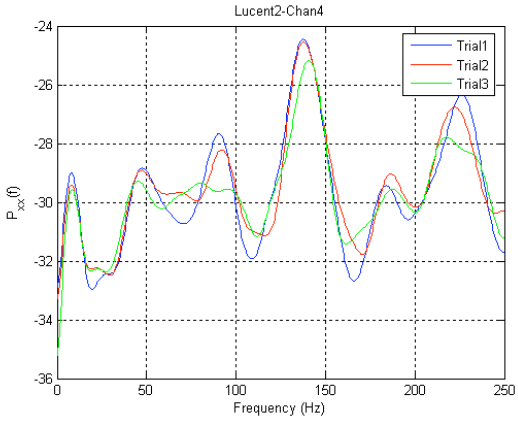
(a)



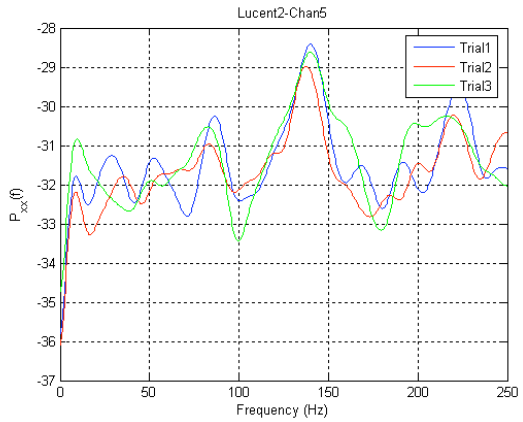
(b)



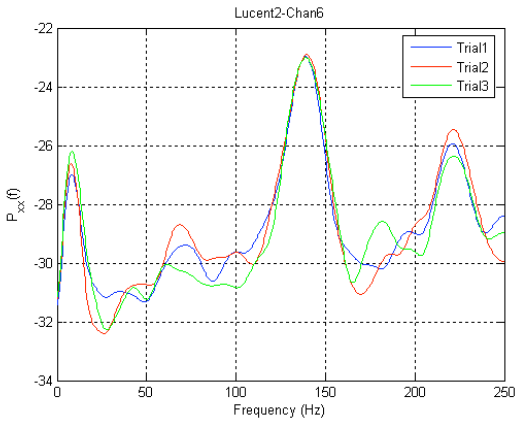
(c)



(d)



(e)

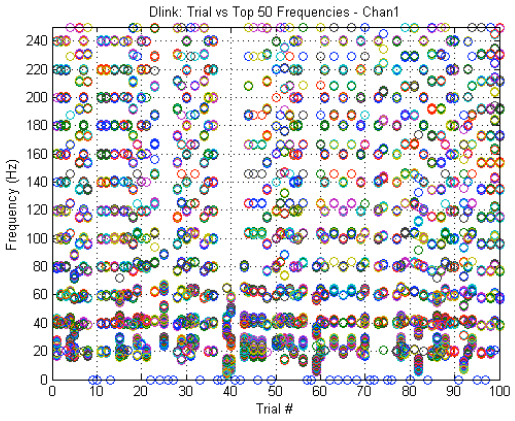


(f)

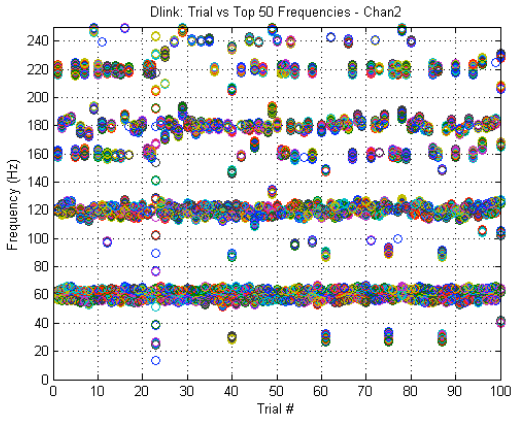
Figure 30 PSDs of Lucent2 card for channels 1 through 6.

APPENDIX B: SCANNING TOP 50 FREQUENCIES

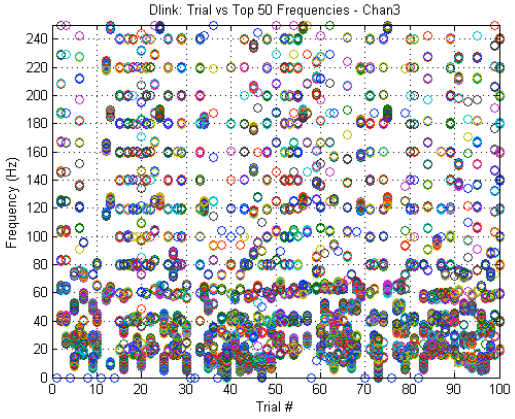
The PSD was calculated for all the experimental trials during our evaluation of the scanning mechanism. This appendix illustrates the frequency ranges that exhibit the greatest magnitude of power within the power spectral density. More specifically, we examine the top 50 frequency points and plot them for comparison between trials on the same channel, trials on different channels, and trials on different wireless cards.



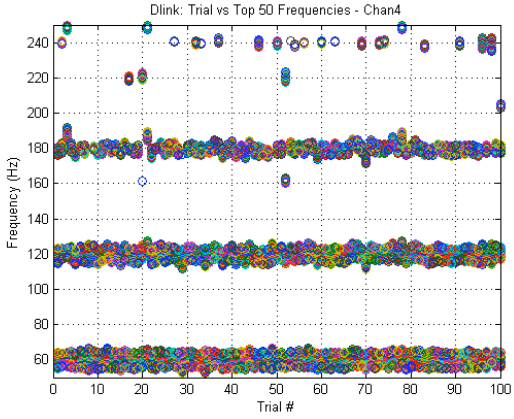
(a)



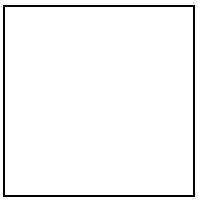
(b)



(c)



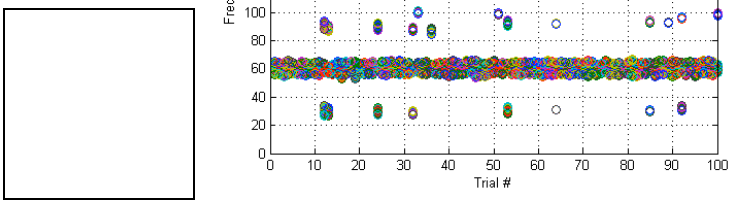
(d)



(e)

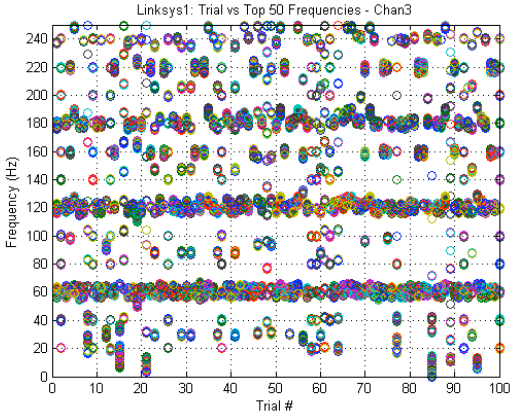
(f)

Figure 31 Top 50 frequencies for DLink card on channels 1 through 6

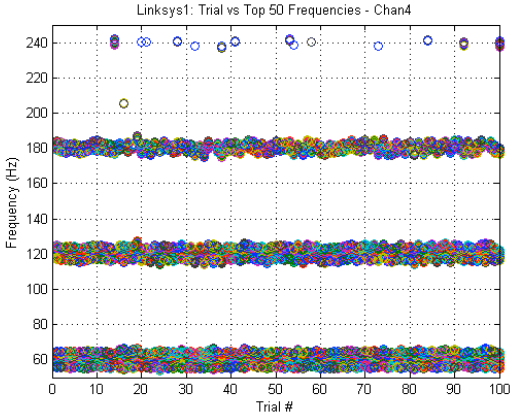


(a)

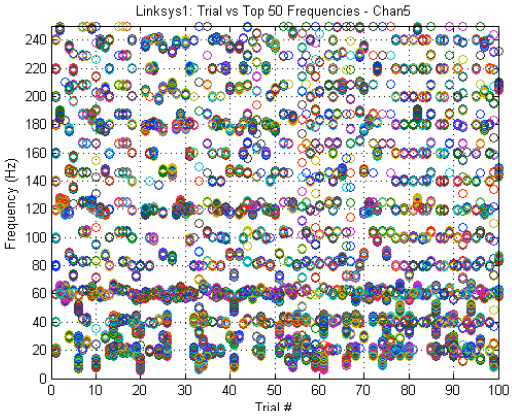
(b)



(c)

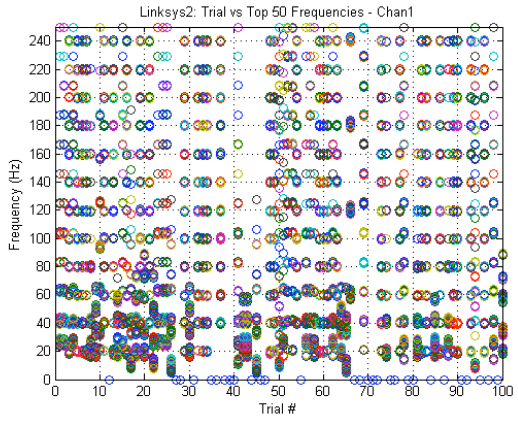


(d)

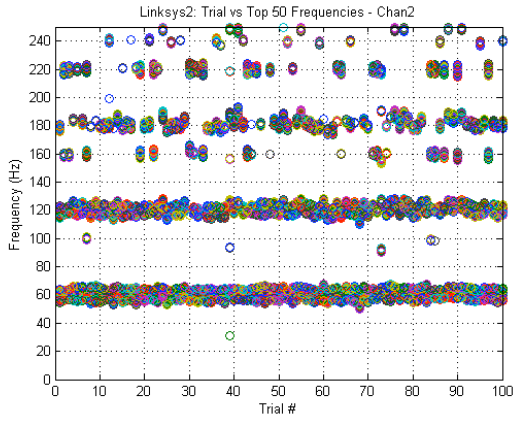


(e)

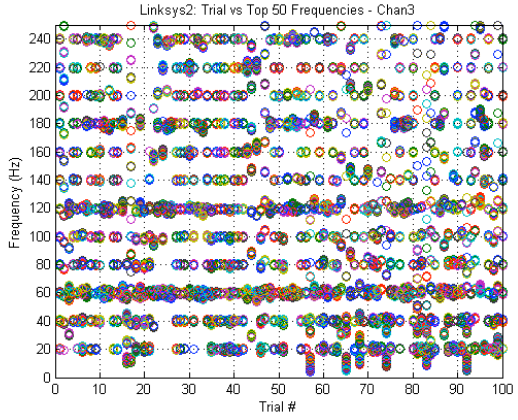
Figure 32 Top 50 frequencies for Linksys1 card on channels 1 through 5



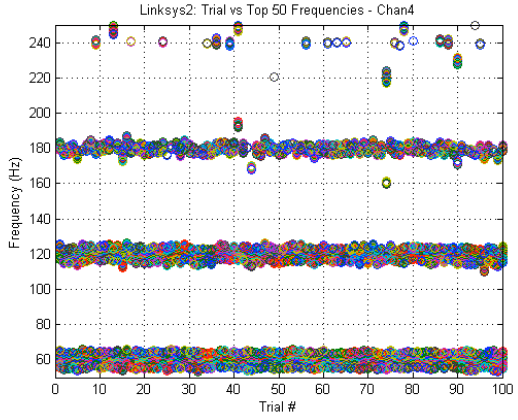
(a)



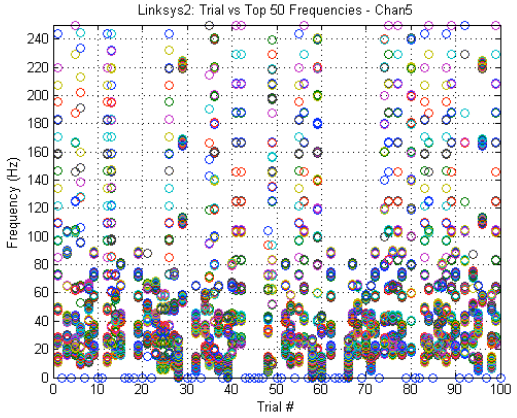
(b)



(c)



(d)



(e)

Figure 33 Top 50 frequencies for Linksys2 card on channels 1 through 5

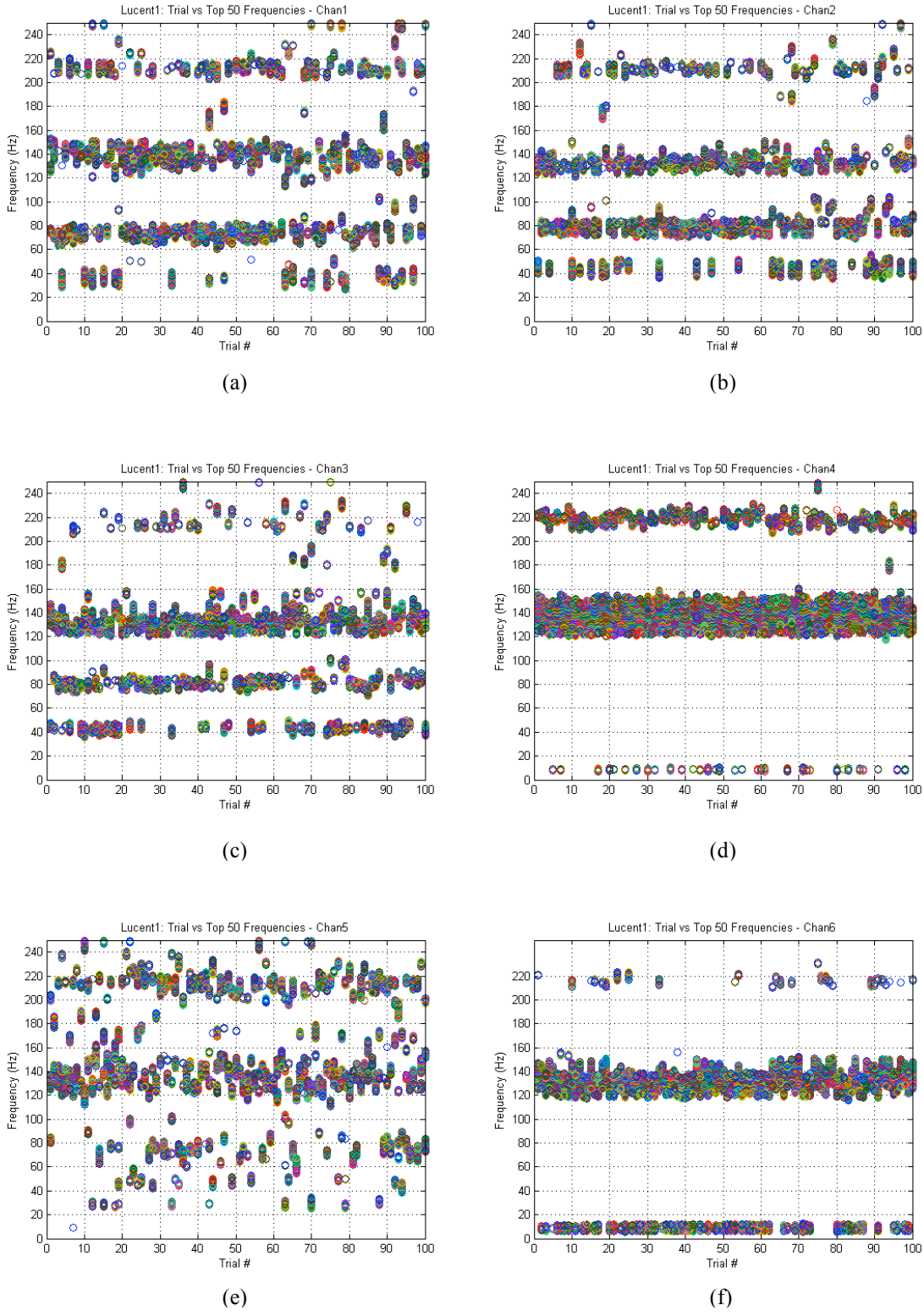
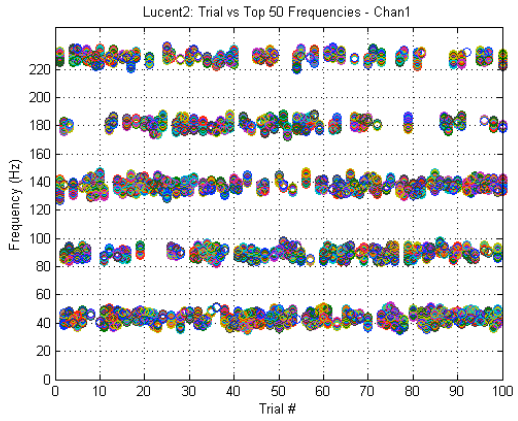
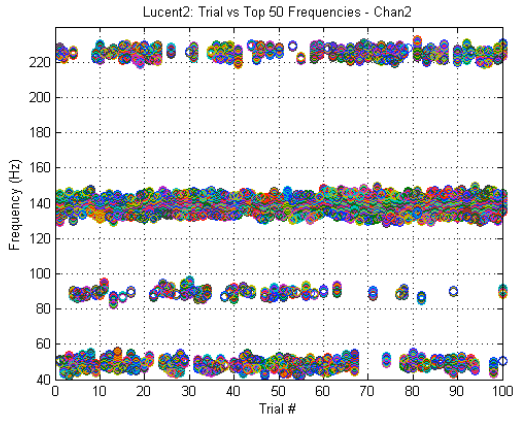


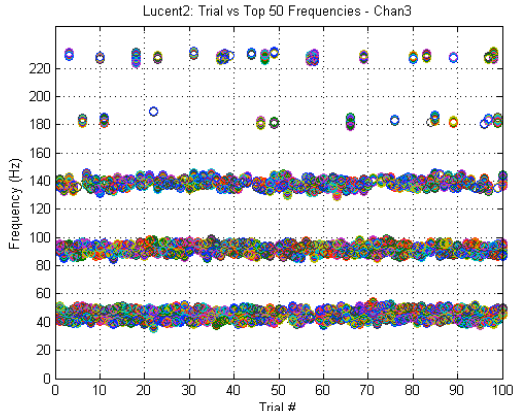
Figure 34 Top 50 frequencies for Lucent1 card on channels 1 through 6



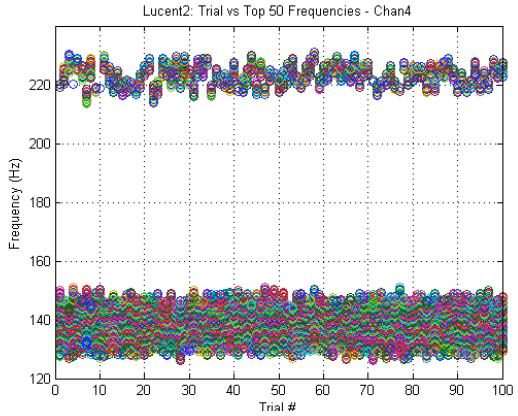
(a)



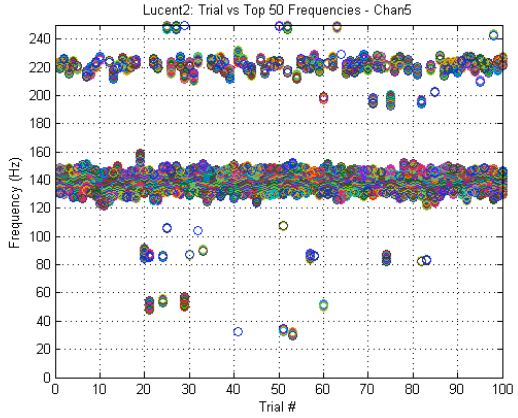
(b)



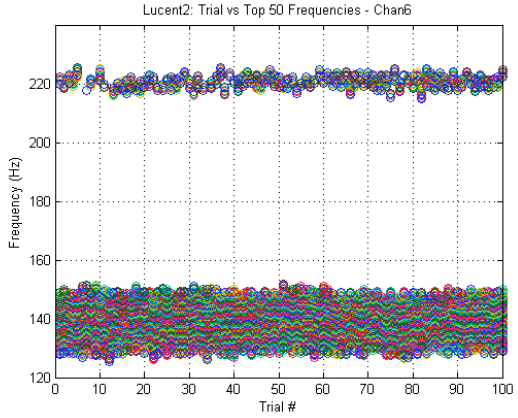
(c)



(d)



(e)



(f)

Figure 35 Top 50 frequencies for Lucent2 card on channels 1 through 6

APPENDIX C: SCANNING SPECTRAL PROFILE

This appendix illustrates the representative spectral profile $F_{\mathbf{R}} = \{f_1, f_2, f_3, \ldots f_{50}\}$ of each NIC per channel for the evaluation of the scanning mechanism.

Table 12 Spectral Profile for Dlink

	F_R Channel 1	F_R Channel 2	F_R Channel 3	F_R Channel 4	F_R Channel 5	F_R Channel 6
f_1	18.555	56.152	15.625	55.176	18.066	55.664
f_2	19.043	56.641	16.113	55.664	18.555	56.152
f_3	19.531	57.129	16.602	56.152	19.043	56.641
f_4	20.02	57.617	17.09	56.641	19.531	57.129
f_5	20.508	58.105	17.578	57.129	20.02	57.617
f_6	20.996	58.594	18.066	57.617	20.508	58.105
f_7	39.063	59.082	18.555	58.105	20.996	58.594
f_8	39.551	59.57	19.043	58.594	21.484	59.082
f_9	40.039	60.059	19.531	59.082	39.551	59.57
f_{10}	40.527	60.547	20.02	59.57	40.039	60.059
f_{11}	59.082	61.035	20.508	60.059	40.527	60.547
f_{12}	59.57	61.523	20.996	60.547	59.57	61.035
f_{13}	60.059	62.012	21.484	61.035	60.059	61.523
f_{14}	60.547	62.5	21.973	61.523	60.547	62.012
f_{15}	79.102	62.988	22.461	62.012	79.102	62.5
f_{16}	79.59	63.477	39.063	62.5	79.59	62.988
f_{17}	80.078	63.965	39.551	62.988	80.078	63.477
f_{18}	80.566	64.453	40.039	63.477	80.566	63.965
f_{19}	99.121	64.941	40.527	63.965	99.121	64.453
f_{20}	99.609	116.7	41.016	64.453	99.609	64.941
f_{21}	100.1	117.19	41.504	115.72	100.1	116.21
f_{22}	100.59	117.68	41.992	116.21	100.59	116.7
f_{23}	119.14	118.16	42.48	116.7	119.14	117.19
f_{24}	119.63	118.65	78.613	117.19	119.63	117.68
f_{25}	120.12	119.14	79.102	117.68	120.12	118.16
f_{26}	120.61	119.63	79.59	118.16	120.61	118.65
f_{27}	139.16	120.12	80.078	118.65	139.16	119.14
f_{28}	139.65	120.61	80.566	119.14	139.65	119.63
f_{29}	140.14	121.09	81.055	119.63	140.14	120.12
f_{30}	140.63	121.58	81.543	120.12	140.63	120.61
f_{31}	159.18	122.07	99.609	120.61	159.18	121.09
f_{32}	159.67	122.56	100.1	121.09	159.67	121.58
f_{33}	160.16	123.05	119.14	121.58	160.16	122.07
f_{34}	160.64	123.54	119.63	122.07	160.64	122.56
f_{35}	179.2	124.02	120.12	122.56	179.2	123.05
f_{36}	179.69	124.51	120.61	123.05	179.69	123.54
f_{37}	180.18	125	139.65	123.54	180.18	124.02
f_{38}	180.66	177.73	140.14	176.27	180.66	124.51
f_{39}	199.22	178.22	140.63	176.76	199.22	178.22
f_{40}	199.71	178.71	159.67	177.25	199.71	178.71
f_{41}	200.2	179.2	160.16	177.73	200.2	179.2
f_{42}	200.68	179.69	160.64	178.22	200.68	179.69
f_{43}	219.24	180.18	179.69	178.71	219.24	180.18
f_{44}	219.73	180.66	180.18	179.2	219.73	180.66
f_{45}	220.21	181.15	199.71	179.69	220.21	181.15
f_{46}	220.7	181.64	200.2	180.18	220.7	181.64
f_{47}	239.26	182.13	219.73	180.66	239.26	182.13
f_{48}	239.75	182.62	220.21	181.15	239.75	182.62
f_{49}	240.23	183.11	239.75	181.64	240.23	183.11
f_{50}	240.72	183.59	240.23	182.13	240.72	183.59

Table 13 Spectral Profile for Linksys1

	F_R Channel 1	F_R Channel 2	F_R Channel 3	F_R Channel 4	F_R Channel 5
f_1	17.578	55.664	56.152	55.664	18.066
f_2	18.066	56.152	56.641	56.152	18.555
f_3	18.555	56.641	57.129	56.641	19.043
f_4	19.043	57.129	57.617	57.129	19.531
f_5	19.531	57.617	58.105	57.617	20.02
f_6	20.02	58.105	58.594	58.105	20.508
f_7	20.508	58.594	59.082	58.594	20.996
f_8	20.996	59.082	59.57	59.082	21.484
f_9	21.484	59.57	60.059	59.57	21.973
f_{10}	39.063	60.059	60.547	60.059	38.574
f_{11}	39.551	60.547	61.035	60.547	39.063
f_{12}	40.039	61.035	61.523	61.035	39.551
f_{13}	40.527	61.523	62.012	61.523	40.039
f_{14}	41.016	62.012	62.5	62.012	40.527
f_{15}	59.082	62.5	62.988	62.5	41.016
f_{16}	59.57	62.988	63.477	62.988	41.504
f_{17}	60.059	63.477	63.965	63.477	41.992
f_{18}	60.547	63.965	64.453	63.965	58.594
f_{19}	61.035	64.453	64.941	64.453	59.082
f_{20}	79.102	64.941	117.19	64.941	59.57
f_{21}	79.59	116.21	117.68	116.7	60.059
f_{22}	80.078	116.7	118.16	117.19	60.547
f_{23}	80.566	117.19	118.65	117.68	61.035
f_{24}	81.055	117.68	119.14	118.16	61.523
f_{25}	99.121	118.16	119.63	118.65	62.012
f_{26}	99.609	118.65	120.12	119.14	79.102
f_{27}	100.1	119.14	120.61	119.63	79.59
f_{28}	100.59	119.63	121.09	120.12	80.078
f_{29}	119.14	120.12	121.58	120.61	80.566
f_{30}	119.63	120.61	122.07	121.09	81.055
f_{31}	120.12	121.09	122.56	121.58	81.543
f_{32}	120.61	121.58	123.05	122.07	82.031
f_{33}	139.16	122.07	123.54	122.56	99.121
f_{34}	139.65	122.56	124.02	123.05	99.609
f_{35}	140.14	123.05	124.51	123.54	100.1
f_{36}	140.63	123.54	125	124.02	100.59
f_{37}	159.67	124.02	125.49	124.51	101.07
f_{38}	160.16	124.51	178.71	177.73	101.56
f_{39}	160.64	177.73	179.2	178.22	102.05
f_{40}	179.69	178.22	179.69	178.71	119.63
f_{41}	180.18	178.71	180.18	179.2	120.12
f_{42}	180.66	179.2	180.66	179.69	120.61
f_{43}	199.71	179.69	181.15	180.18	121.09
f_{44}	200.2	180.18	181.64	180.66	121.58
f_{45}	200.68	180.66	182.13	181.15	122.07
f_{46}	219.73	181.15	182.62	181.64	140.14
f_{47}	220.21	181.64	183.11	182.13	140.63
f_{48}	220.7	182.13	183.59	182.62	141.11
f_{49}	239.75	182.62	184.08	183.11	141.6
f_{50}	240.23	183.11	184.57	183.59	160.64

Table 14 Spectral Profile for Linksys2

	F_R Channel 1	F_R Channel 2	F_R Channel 3	F_R Channel 4	F_R Channel 5
f_1	20.02	56.152	55.664	55.176	15.625
f_2	20.508	56.641	56.152	55.664	16.113
f_3	39.063	57.129	56.641	56.152	16.602
f_4	39.551	57.617	57.129	56.641	17.09
f_5	40.039	58.105	57.617	57.129	17.578
f_6	40.527	58.594	58.105	57.617	18.066
f_7	41.016	59.082	58.594	58.105	18.555
f_8	59.082	59.57	59.082	58.594	19.043
f_9	59.57	60.059	59.57	59.082	19.531
f_{10}	60.059	60.547	60.059	59.57	20.02
f_{11}	60.547	61.035	60.547	60.059	20.508
f_{12}	61.035	61.523	61.035	60.547	20.996
f_{13}	79.102	62.012	61.523	61.035	21.484
f_{14}	79.59	62.5	62.012	61.523	21.973
f_{15}	80.078	62.988	62.5	62.012	22.461
f_{16}	80.566	63.477	62.988	62.5	22.949
f_{17}	81.055	63.965	63.477	62.988	31.25
f_{18}	99.121	64.453	63.965	63.477	31.738
f_{19}	99.609	64.941	64.453	63.965	32.227
f_{20}	100.1	65.43	64.941	64.453	32.715
f_{21}	100.59	117.68	116.7	115.23	33.203
f_{22}	101.07	118.16	117.19	115.72	33.691
f_{23}	119.14	118.65	117.68	116.21	34.18
f_{24}	119.63	119.14	118.16	116.7	34.668
f_{25}	120.12	119.63	118.65	117.19	35.156
f_{26}	120.61	120.12	119.14	117.68	35.645
f_{27}	139.16	120.61	119.63	118.16	36.133
f_{28}	139.65	121.09	120.12	118.65	36.621
f_{29}	140.14	121.58	120.61	119.14	37.109
f_{30}	140.63	122.07	121.09	119.63	37.598
f_{31}	159.18	122.56	121.58	120.12	56.641
f_{32}	159.67	123.05	122.07	120.61	57.129
f_{33}	160.16	123.54	122.56	121.09	57.617
f_{34}	160.64	124.02	123.05	121.58	58.105
f_{35}	179.2	124.51	123.54	122.07	58.594
f_{36}	179.69	125	124.02	122.56	59.082
f_{37}	180.18	125.49	124.51	123.05	71.289
f_{38}	180.66	125.98	125	123.54	71.777
f_{39}	199.22	180.18	178.22	176.76	72.266
f_{40}	199.71	180.66	178.71	177.25	72.754
f_{41}	200.2	181.15	179.2	177.73	73.242
f_{42}	200.68	181.64	179.69	178.22	73.73
f_{43}	219.24	182.13	180.18	178.71	74.219
f_{44}	219.73	182.62	180.66	179.2	74.707
f_{45}	220.21	183.11	181.15	179.69	75.195
f_{46}	220.7	183.59	181.64	180.18	87.402
f_{47}	239.26	184.08	182.13	180.66	87.891
f_{48}	239.75	184.57	182.62	181.15	88.379
f_{49}	240.23	185.06	183.11	181.64	88.867
f_{50}	240.72	185.55	183.59	182.13	89.355

Table 15 Spectral Profile for Lucent1

	F_R Channel 1	F_R Channel 2	F_R Channel 3	F_R Channel 4	F_R Channel 5	F_R Channel 6
f_1	68.848	79.59	77.637	126.46	126.46	124.51
f_2	69.336	80.078	78.125	126.95	126.95	125
f_3	69.824	80.566	78.613	127.44	127.44	125.49
f_4	70.313	81.055	79.102	127.93	127.93	125.98
f_5	70.801	81.543	79.59	128.42	128.42	126.46
f_6	71.289	82.031	80.078	128.91	128.91	126.95
f_7	71.777	82.52	80.566	129.39	129.39	127.44
f_8	72.266	83.008	81.055	129.88	129.88	127.93
f_9	72.754	83.496	81.543	130.37	130.37	128.42
f_{10}	73.242	83.984	82.031	130.86	130.86	128.91
f_{11}	73.73	84.473	82.52	131.35	131.35	129.39
f_{12}	74.219	84.961	83.008	131.84	131.84	129.88
f_{13}	74.707	85.449	83.496	132.32	132.32	130.37
f_{14}	75.195	85.938	83.984	132.81	132.81	130.86
f_{15}	75.684	86.426	84.473	133.3	133.3	131.35
f_{16}	76.172	86.914	84.961	133.79	133.79	131.84
f_{17}	76.66	87.402	85.449	134.28	134.28	132.32
f_{18}	77.148	128.91	85.938	134.77	134.77	132.81
f_{19}	77.637	129.39	86.426	135.25	135.25	133.3
f_{20}	78.125	129.88	86.914	135.74	135.74	133.79
f_{21}	78.613	130.37	122.07	136.23	136.23	134.28
f_{22}	133.3	130.86	122.56	136.72	136.72	134.77
f_{23}	133.79	131.35	123.05	137.21	137.21	135.25
f_{24}	134.28	131.84	123.54	137.7	137.7	135.74
f_{25}	134.77	132.32	124.02	138.18	138.18	136.23
f_{26}	135.25	132.81	124.51	138.67	138.67	136.72
f_{27}	135.74	133.3	125	139.16	139.16	137.21
f_{28}	136.23	133.79	125.49	139.65	139.65	137.7
f_{29}	136.72	134.28	125.98	140.14	140.14	138.18
f_{30}	137.21	134.77	126.46	140.63	140.63	138.67
f_{31}	137.7	135.25	126.95	141.11	141.11	139.16
f_{32}	138.18	135.74	127.44	141.6	141.6	139.65
f_{33}	138.67	136.23	127.93	142.09	142.09	140.14
f_{34}	139.16	136.72	128.42	142.58	142.58	140.63
f_{35}	139.65	137.21	128.91	143.07	143.07	141.11
f_{36}	140.14	137.7	129.39	143.55	143.55	141.6
f_{37}	140.63	138.18	129.88	144.04	144.04	142.09
f_{38}	141.11	138.67	130.37	144.53	144.53	142.58
f_{39}	141.6	139.16	130.86	145.02	145.02	143.07
f_{40}	142.09	139.65	131.35	145.51	211.91	143.55
f_{41}	142.58	140.14	131.84	146	212.4	144.04
f_{42}	143.07	140.63	132.32	221.19	212.89	144.53
f_{43}	143.55	141.11	132.81	221.68	213.38	145.02
f_{44}	144.04	141.6	133.3	222.17	213.87	145.51
f_{45}	144.53	142.09	133.79	222.66	214.36	146
f_{46}	145.02	142.58	134.28	223.14	214.84	146.48
f_{47}	145.51	143.07	134.77	223.63	215.33	146.97
f_{48}	146	143.55	135.25	224.12	215.82	147.46
f_{49}	146.48	144.04	135.74	224.61	216.31	147.95
f_{50}	146.97	144.53	136.23	225.1	216.8	148.44

Table 16 Spectral Profile for Lucent2

	F_R Channel 1	F_R Channel 2	F_R Channel 3	F_R Channel 4	F_R Channel 5	F_R Channel 6
f_1	36.621	44.922	41.016	131.84	133.79	129.39
f_2	37.109	45.41	41.504	132.32	134.28	129.88
f_3	37.598	45.898	41.992	132.81	134.77	130.37
f_4	38.086	46.387	42.48	133.3	135.25	130.86
f_5	38.574	46.875	42.969	133.79	135.74	131.35
f_6	39.063	47.363	43.457	134.28	136.23	131.84
f_7	39.551	47.852	43.945	134.77	136.72	132.32
f_8	40.039	48.34	44.434	135.25	137.21	132.81
f_9	40.527	48.828	44.922	135.74	137.7	133.3
f_{10}	41.016	49.316	45.41	136.23	138.18	133.79
f_{11}	41.504	49.805	45.898	136.72	138.67	134.28
f_{12}	41.992	50.293	46.387	137.21	139.16	134.77
f_{13}	42.48	50.781	46.875	137.7	139.65	135.25
f_{14}	42.969	51.27	47.363	138.18	140.14	135.74
f_{15}	43.457	132.81	47.852	138.67	140.63	136.23
f_{16}	43.945	133.3	48.34	139.16	141.11	136.72
f_{17}	44.434	133.79	48.828	139.65	141.6	137.21
f_{18}	44.922	134.28	49.316	140.14	142.09	137.7
f_{19}	45.41	134.77	88.867	140.63	142.58	138.18
f_{20}	45.898	135.25	89.355	141.11	143.07	138.67
f_{21}	46.387	135.74	89.844	141.6	143.55	139.16
f_{22}	46.875	136.23	90.332	142.09	144.04	139.65
f_{23}	47.363	136.72	90.82	142.58	144.53	140.14
f_{24}	47.852	137.21	91.309	143.07	145.02	140.63
f_{25}	48.34	137.7	91.797	143.55	145.51	141.11
f_{26}	48.828	138.18	92.285	144.04	146	141.6
f_{27}	86.914	138.67	92.773	144.53	146.48	142.09
f_{28}	87.402	139.16	93.262	145.02	146.97	142.58
f_{29}	87.891	139.65	93.75	145.51	147.46	143.07
f_{30}	88.379	140.14	94.238	146	147.95	143.55
f_{31}	88.867	140.63	94.727	146.48	148.44	144.04
f_{32}	89.355	141.11	134.77	146.97	216.31	144.53
f_{33}	89.844	141.6	135.25	147.46	216.8	145.02
f_{34}	90.332	221.19	135.74	147.95	217.29	145.51
f_{35}	90.82	221.68	136.23	148.44	217.77	146
f_{36}	91.309	222.17	136.72	148.93	218.26	146.48
f_{37}	91.797	222.66	137.21	149.41	218.75	146.97
f_{38}	134.28	223.14	137.7	218.75	219.24	147.46
f_{39}	134.77	223.63	138.18	219.24	219.73	217.77
f_{40}	135.25	224.12	138.67	219.73	220.21	218.26
f_{41}	135.74	224.61	139.16	220.21	220.7	218.75
f_{42}	136.23	225.1	139.65	220.7	221.19	219.24
f_{43}	136.72	225.59	140.14	221.19	221.68	219.73
f_{44}	137.21	226.07	140.63	221.68	222.17	220.21
f_{45}	137.7	226.56	141.11	222.17	222.66	220.7
f_{46}	138.18	227.05	141.6	222.66	223.14	221.19
f_{47}	138.67	227.54	142.09	223.14	223.63	221.68
f_{48}	139.16	228.03	142.58	223.63	224.12	222.17
f_{49}	139.65	228.52	143.07	224.12	224.61	222.66
f_{50}	140.14	229	143.55	224.61	225.1	223.14

APPENDIX D: SCANNING COMPARISON RESULTS

This appendix illustrates the results of comparing the spectral profile of experimental trials with the spectral profile $F_{\mathbf{R}}$ that represents the signature of the NIC. Comparisons are done per channel.

Table 17 Dlink Channel 1

Frequency Range (Hz)	Percent of F_R	Percent Match
18.555 - 20.996	12%	44%
39.063 - 40.527	8%	65%
59.082 - 60.547	8%	31%
79.102 - 80.566	8%	30%
99.121 - 100.59	8%	26%
119.14 - 120.61	8%	26%
139.16 - 140.63	8%	26%
159.18 - 160.64	8%	26%
179.2 - 180.66	8%	26%
199.22 - 200.68	8%	26%
219.24 - 220.7	8%	27%
239.26 - 240.72	8%	26%
All		19%

Table 18 Dlink Channel 2

Frequency Range (Hz)	Percent of F_R	Percent Match
56.152 - 64.941	38%	100%
116.7 - 125	36%	95%
177.73 - 183.59	26%	62%
All		61%

Table 19 Dlink Channel 3

Frequency Range (Hz)	Percent of F_R	Percent Match
15.625 - 22.461	30%	48%
39.063 - 42.48	16%	49%
78.613 - 81.543	14%	31%
99.609 - 100.1	4%	23%
119.14 - 120.61	8%	31%
139.65 - 140.63	6%	21%
159.67 - 160.64	6%	26%
179.69 - 180.18	4%	23%
199.71 - 200.2	4%	20%
219.73 - 220.21	4%	25%
239.75 - 240.23	4%	19%
All		18%

Table 20 Dlink Channel 4

Frequency Range (Hz)	Percent of F_R	Percent Match
55.176 - 64.453	40%	100%
115.72 - 123.54	34%	100%
176.27 - 182.13	26%	90%
All		90%

Table 21 Dlink Channel 5

Frequency Range (Hz)	Percent of F_R	Percent Match
18.066 - 21.484	16%	53%
39.551 - 40.527	6%	57%
59.57 - 60.547	6%	64%
79.102 - 80.566	8%	38%
99.121 - 100.59	8%	44%
119.14 - 120.61	8%	59%
139.16 - 140.63	8%	35%
159.18 - 160.64	8%	50%
179.2 - 180.66	8%	51%
199.22 - 200.68	8%	39%
219.24 - 220.7	8%	52%
239.26 - 240.72	8%	47%
All		23%

Table 22 Dlink Channel 6

Frequency Range (Hz)	Percent of F_R	Percent Match
55.664 - 64.941	40%	100%
116.21 - 124.51	36%	100%
178.22 - 183.59	24%	99%
All		99%

Table 23 Linksys1 Channel 1

Frequency Range (Hz)	Percent of F_R	Percent Match
17.578 - 21.484	18%	41%
39.063 - 41.016	10%	46%
59.082 - 61.035	10%	27%
79.102 - 81.055	10%	22%
99.121 - 100.59	8%	16%
119.14 - 120.61	8%	19%
139.16 - 140.63	8%	17%
159.67 - 160.64	6%	19%
179.69 - 180.66	6%	16%
199.71 - 200.68	6%	15%
219.73 - 220.7	6%	18%
239.75 - 240.23	4%	17%
All		13%

Table 24 Linksys1 Channel 2

Frequency Range (Hz)	Percent of F_R	Percent Match
55.664 - 64.941	40%	100%
116.21 - 124.51	36%	100%
177.73 - 183.11	24%	84%
All		84%

Table 25 Linksys1 Channel 3

Frequency Range (Hz)	Percent of F_R	Percent Match
56.152 - 64.941	38%	97%
117.19 - 125.49	36%	91%
178.71 - 184.57	26%	65%
All		62%

Table 26 Linksys1 Channel 4

Frequency Range (Hz)	Percent of F_R	Percent Match
55.664 - 64.941	40%	100%
116.7 - 124.51	34%	100%
177.73 - 183.59	26%	97%
All		97%

Table 27 Linksys1 Channel 5

Frequency Range (Hz)	Percent of F_R	Percent Match
18.066 - 21.973	18%	45%
38.574 - 41.992	16%	60%
58.594 - 62.012	16%	91%
79.102 - 82.031	14%	30%
99.121 - 102.05	14%	30%
119.63 - 122.07	12%	47%
140.14 - 141.6	8%	21%
160.64 - 160.64	2%	25%
All		16%

Table 28 Linksys2 Channel 1

Frequency Range (Hz)	Percent of F_R	Percent Match
20.02 - 20.508	4%	44%
39.063 - 41.016	10%	59%
59.082 - 61.035	10%	37%
79.102 - 81.055	10%	34%
99.121 - 101.07	10%	34%
119.14 - 120.61	8%	35%
139.16 - 140.63	8%	34%
159.18 - 160.64	8%	35%
179.2 - 180.66	8%	35%
199.22 - 200.68	8%	32%
219.24 - 220.7	8%	33%
239.26 - 240.72	8%	35%
All		28%

Table 29 Linksys2 Channel 2

Frequency Range (Hz)	Percent of F_R	Percent Match
56.152 - 65.43	40%	100%
117.68 - 125.98	36%	97%
180.18 - 185.55	24%	68%
All		68%

Table 30 Linksys2 Channel 3

Frequency Range (Hz)	Percent of F_R	Percent Match
55.664 - 64.941	40%	95%
116.7 - 125	36%	91%
178.22 - 183.59	24%	59%
All		55%

Table 31 Linksys2 Channel 4

Frequency Range (Hz)	Percent of F_R	Percent Match
55.176 - 64.453	40%	100%
115.23 - 123.54	36%	100%
176.76 - 182.13	24%	94%
All		94%

Table 32 Linksys2 Channel 5

Frequency Range (Hz)	Percent of F_R	Percent Match
15.625 - 22.949	32%	31%
31.25 - 37.598	28%	23%
56.641 - 59.082	12%	17%
71.289 - 75.195	18%	19%
87.402 - 89.355	10%	10%
All		6%

Table 33 Lucent1 Channel 1

Frequency Range (Hz)	Percent of F_R	Percent Match
68.848 - 78.613	42%	73%
133.3 - 146.97	58%	78%
All		63%

Table 34 Lucent1 Channel 2

Frequency Range (Hz)	Percent of F_R	Percent Match
79.59 - 87.402	34%	79%
128.91 - 144.53	66%	90%
All		75%

Table 35 Lucent1 Channel 3

Frequency Range (Hz)	Percent of F_R	Percent Match
77.637 - 86.914	40%	75%
122.07 - 136.23	60%	91%
All		70%

Table 36 Lucent1 Channel 4

Frequency Range (Hz)	Percent of F_R	Percent Match
126.46 - 146	82%	100%
221.19 - 225.1	18%	90%
All		90%

Table 37 Lucent1 Channel 5

Frequency Range (Hz)	Percent of F_R	Percent Match
126.46 - 145.02	78%	90%
211.91 - 216.8	22%	49%
All		44%

Table 38 Lucent1 Channel 6

Frequency Range (Hz)	Percent of F_R	Percent Match
124.51 - 148.44	100%	100%
All		100%

Table 39 Lucent2 Channel 1

Frequency Range (Hz)	Percent of F_R	Percent Match
36.621 - 48.828	52%	81%
86.914 - 91.797	22%	62%
134.28 - 140.14	26%	76%
All		33%

Table 40 Lucent2 Channel 2

Frequency Range (Hz)	Percent of F_R	Percent Match
44.922 - 51.27	28%	73%
132.81 - 141.6	38%	100%
221.19 - 229	34%	65%
All		38%

Table 41 Lucent2 Channel 3

Frequency Range (Hz)	Percent of F_R	Percent Match
41.016 - 49.316	36%	98%
88.867 - 94.727	26%	98%
134.77 - 143.55	38%	94%
All		38%

Table 42 Lucent2 Channel 4

Frequency Range (Hz)	Percent of F_R	Percent Match
131.84 - 149.41	74%	100%
218.75 - 224.61	26%	94%
All		94%

Table 43 Lucent2 Channel 5

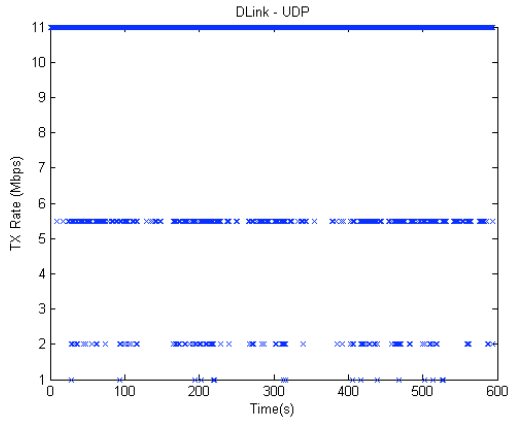
Frequency Range (Hz)	Percent of F_R	Percent Match
133.79 - 148.44	62%	100%
216.31 - 225.1	38%	73%
All		73%

Table 44 Lucent2 Channel 6

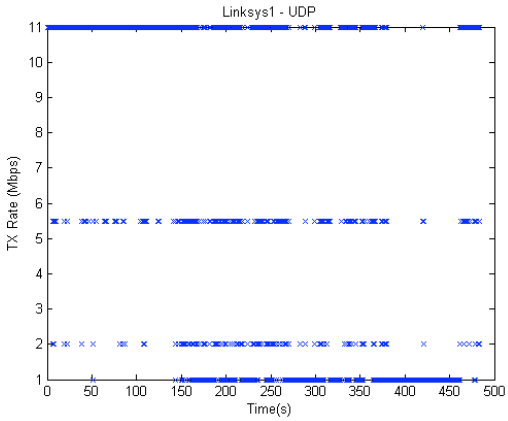
Frequency Range (Hz)	Percent of F_R	Percent Match
129.39 - 147.46	76%	100%
217.77 - 223.14	24%	94%
All		94%

APPENDIX E: RATE SWITCHING TRANSMISSION RATE

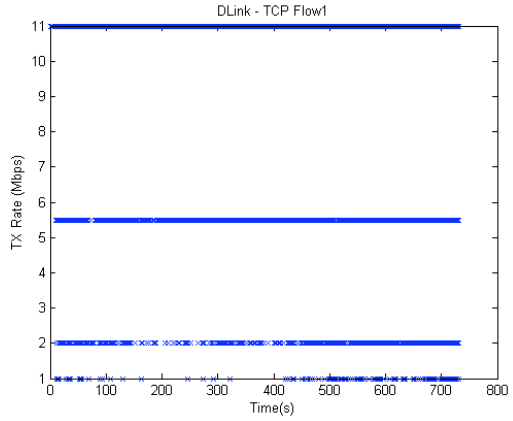
This appendix illustrates NICs invoking rate switching during UDP and TCP session in a real environment.



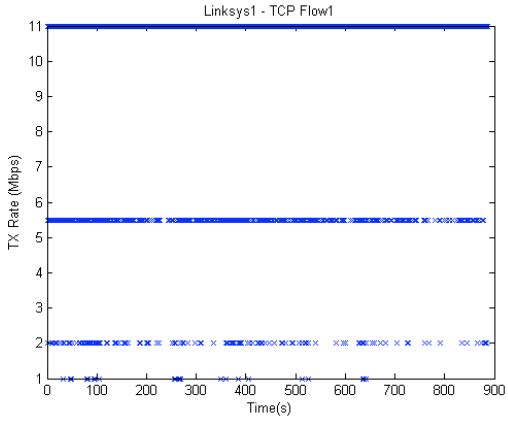
(a)



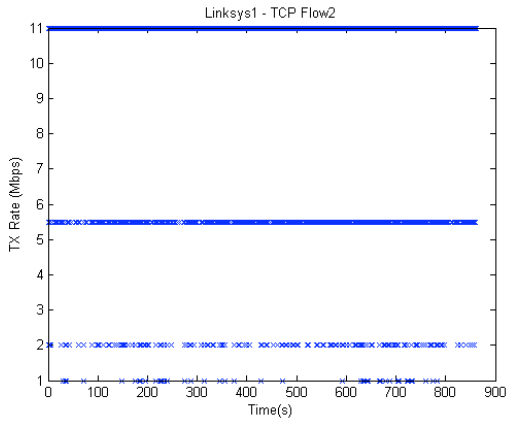
(b)



(c)



(d)



(e)

Figure 36 Dlink and Linksys1 invoking rate switching

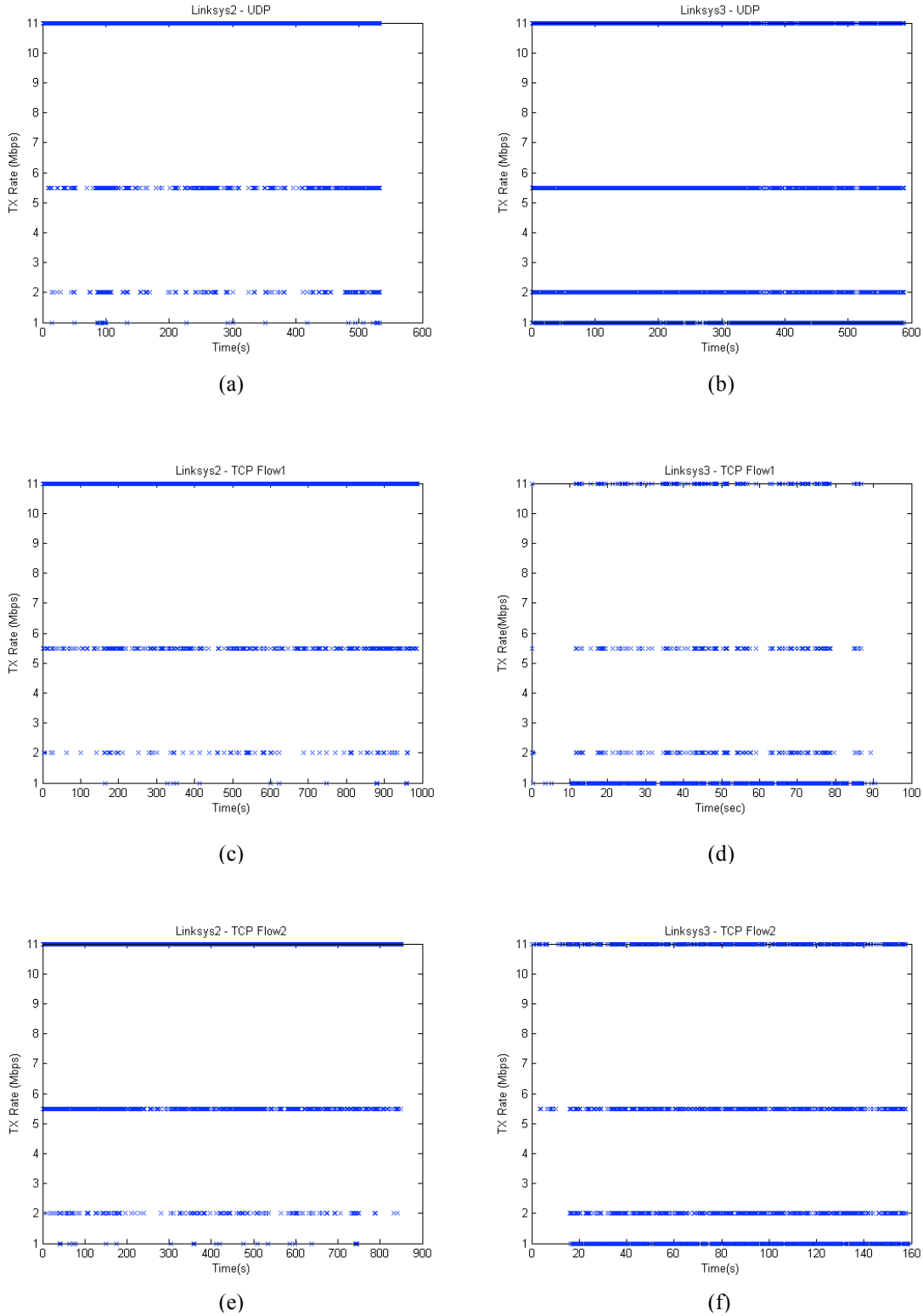


Figure 37 Linksys2 and Linksys3 invoking rate switching

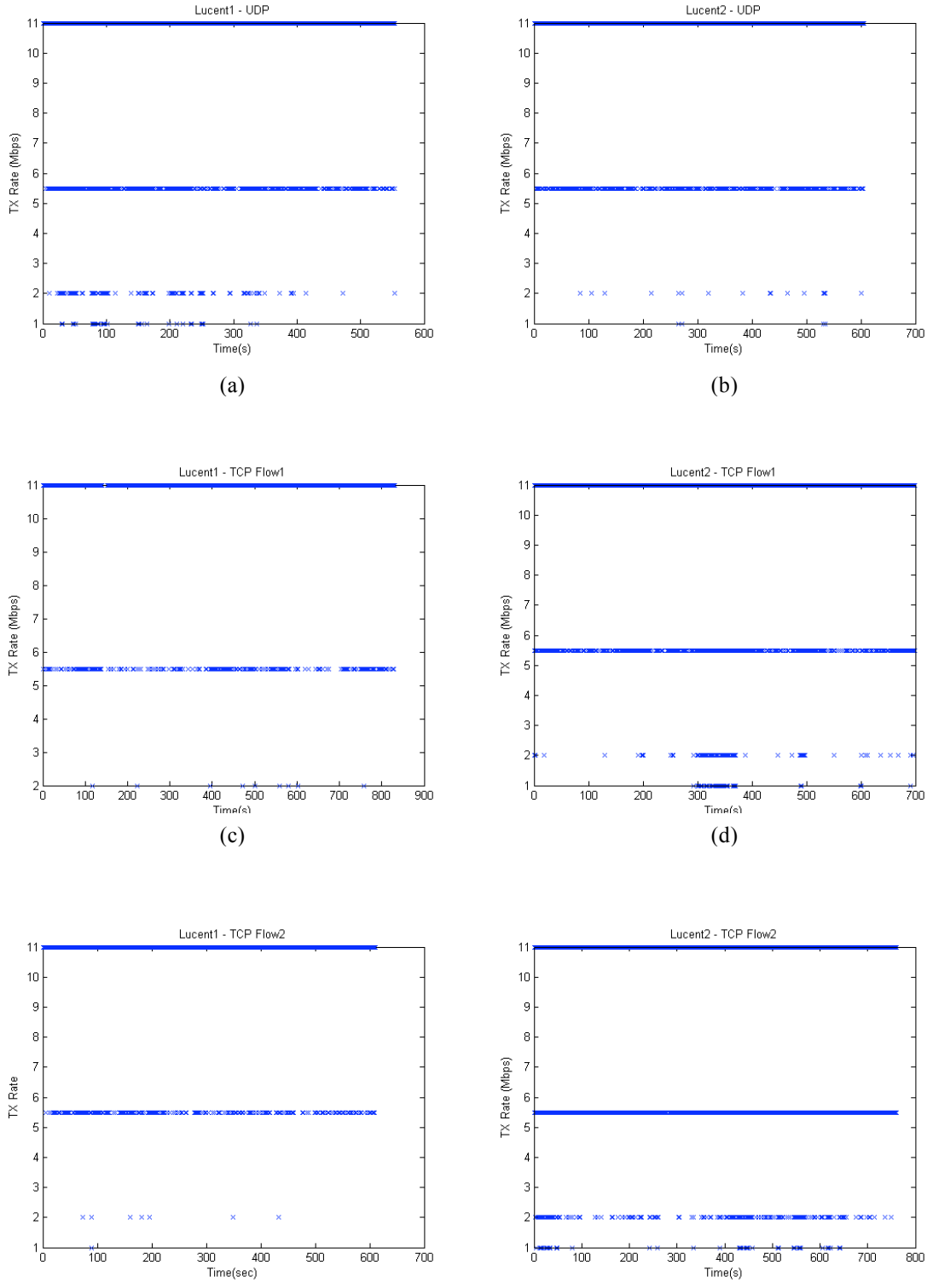
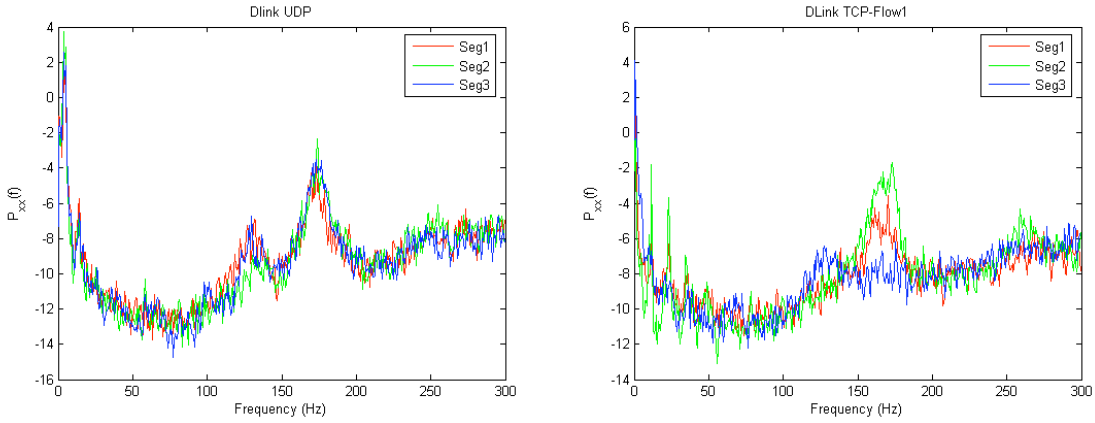


Figure 38 Lucent1 and Lucent2 invoking rate switching

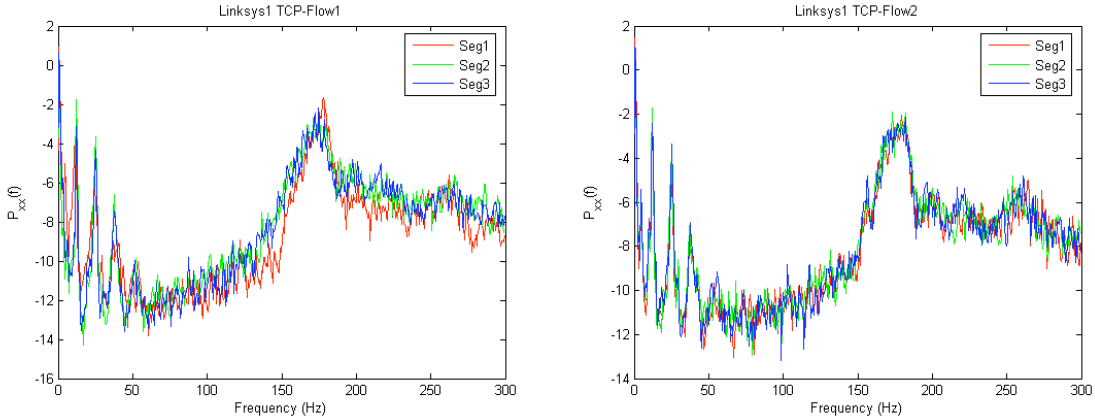
APPENDIX F: RATE SWITCHING POWER SPECTRAL DENSITY PLOTS

This appendix contains excerpt of plots illustrating the PSD of the communication traffic generated from rate switching mechanism of the NICs. Each graph plots the PSD of first three 60-second segments of a traffic flow for each traffic type on each NIC.

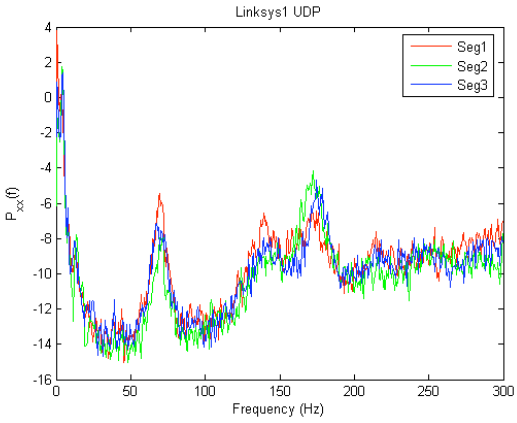


(a) (b)

Figure 39 PSD of Dlink during rate switching

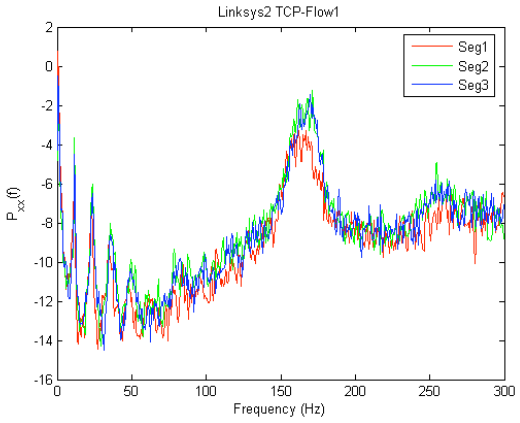


(a) (b)

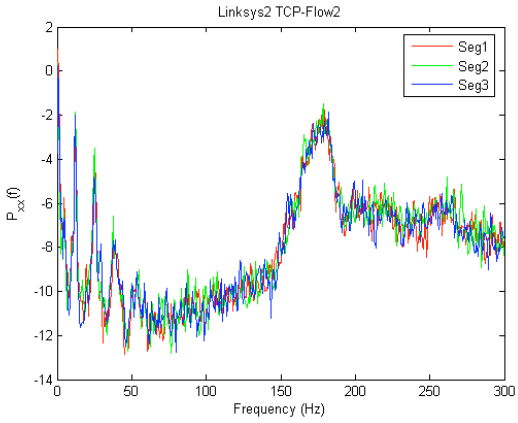


(c)

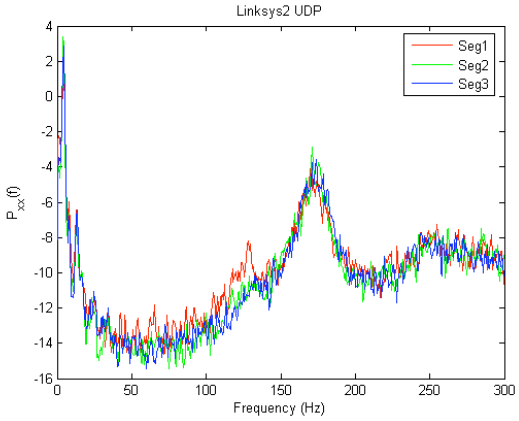
Figure 40 PSD of Linksys1 card during rate switching



(a)

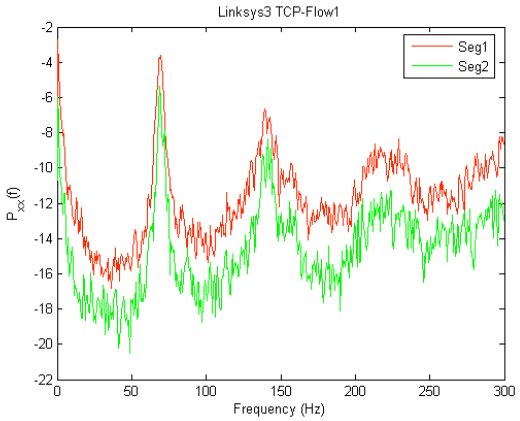


(b)

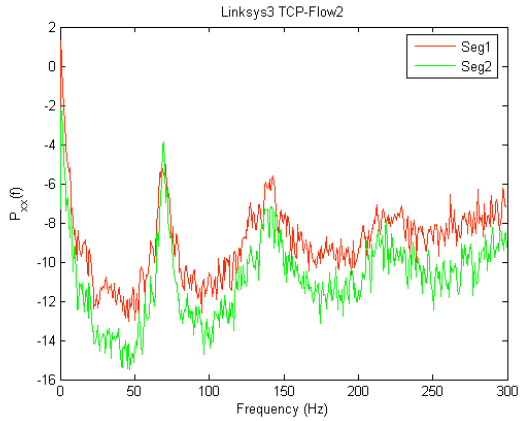


(c)

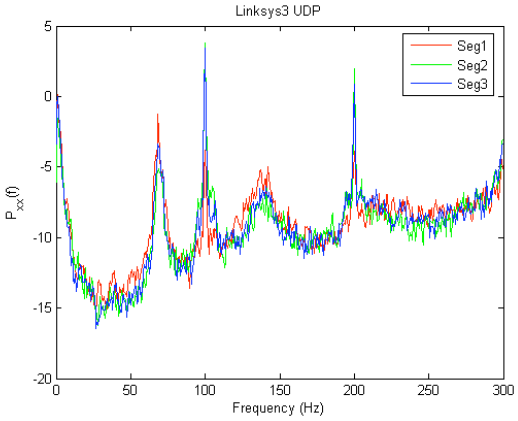
Figure 41 PSD of Linksys2 card during rate switching



(a)

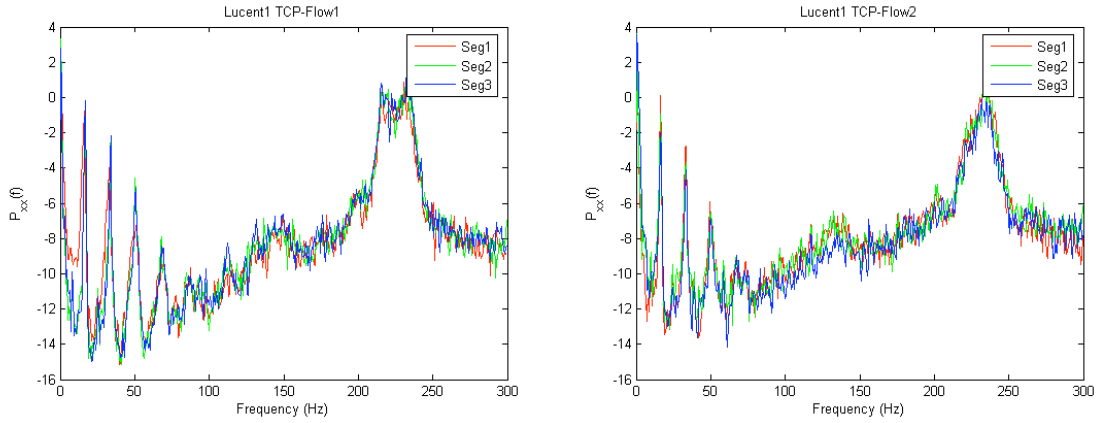


(b)

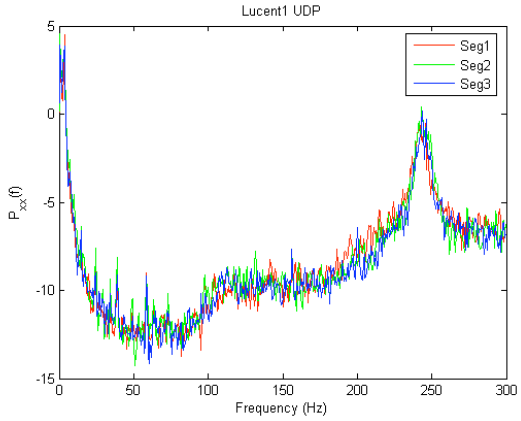


(c)

Figure 42 PSD of Linksys3 card during rate switching

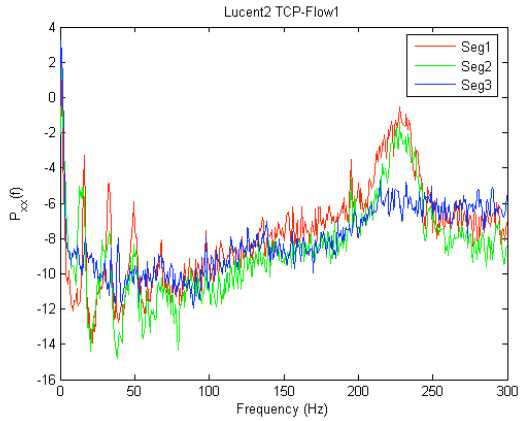


(a) (b)

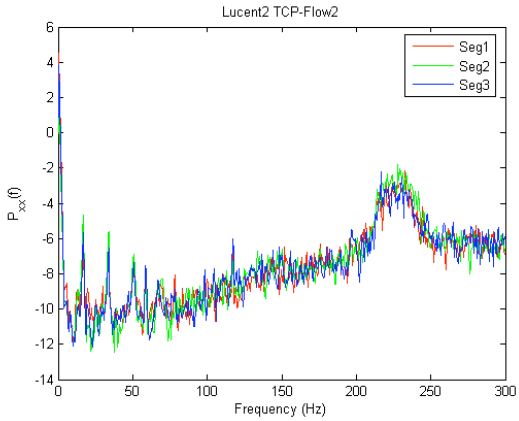


(c)

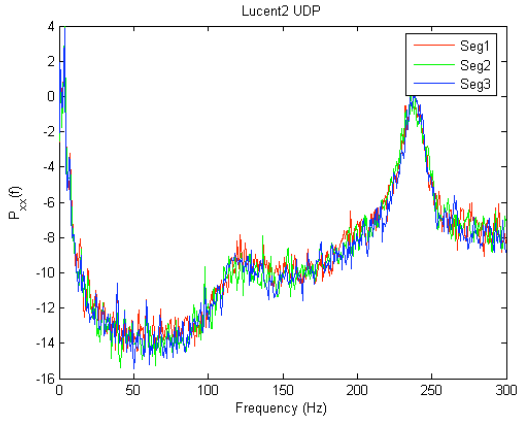
Figure 43 PSD of Lucent1 card during rate switching



(a)



(b)

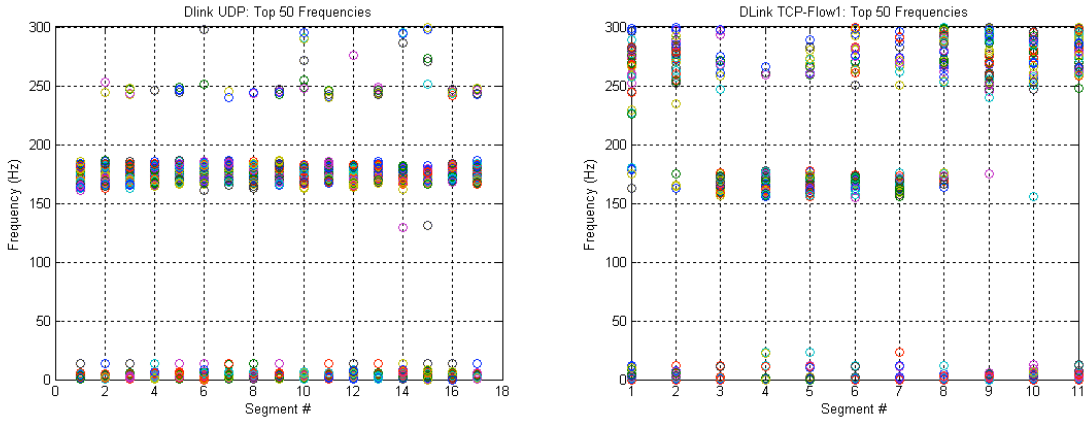


(c)

Figure 44 PSD of Lucent2 card during rate switching

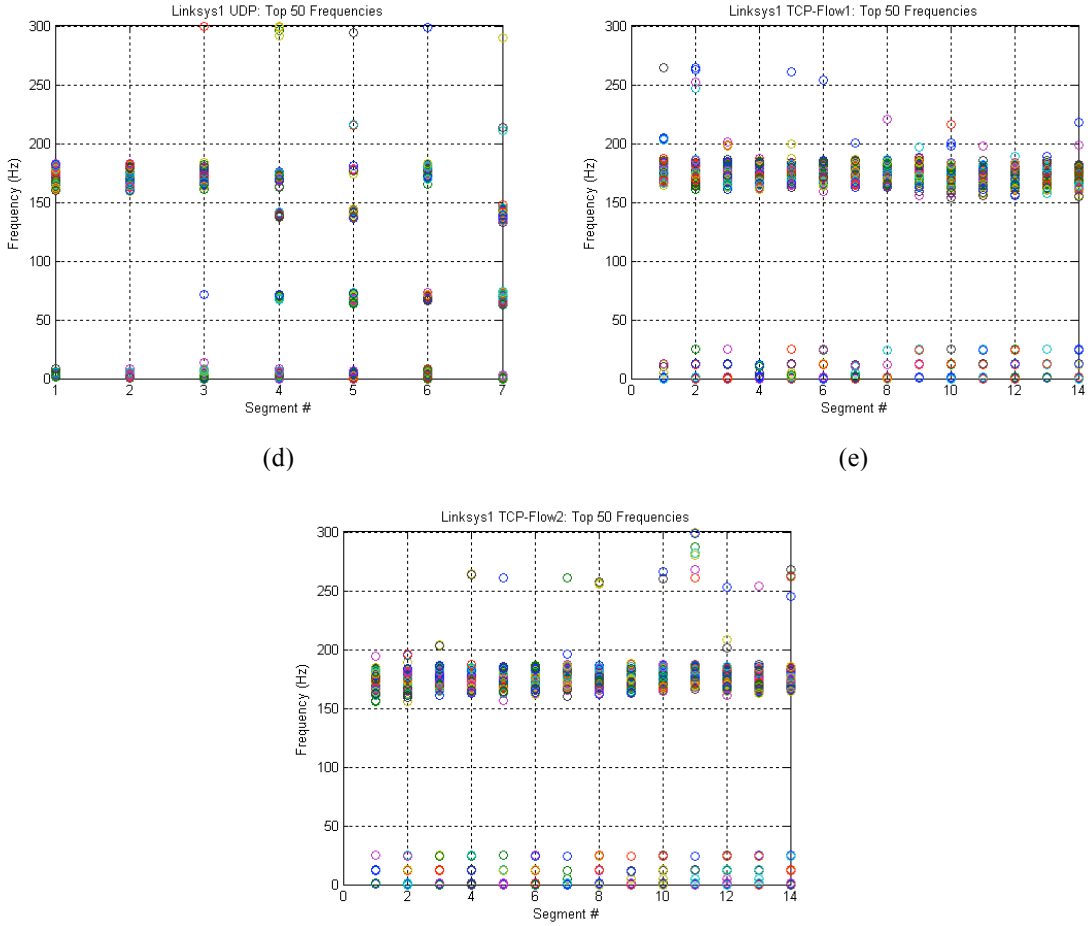
APPENDIX G: RATE SWITCHING TOP 50 FREQUENCIES

The PSD was calculated for 60-second segments of traffic flow while the NIC was invoking rate switching. This appendix illustrates the frequency ranges that exhibit the greatest magnitude of power within the power spectral density. More specifically, we examine the top 50 frequency points and plot them.



(a) (b)

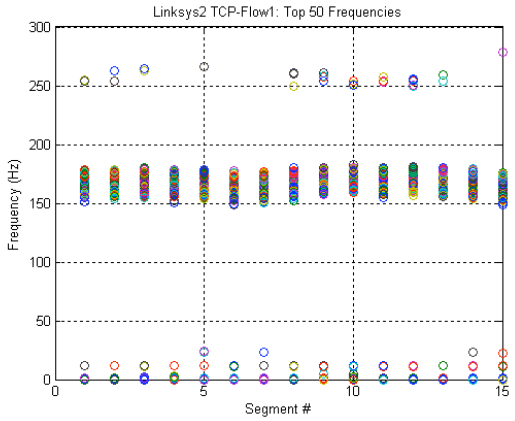
Figure 45 Top 50 frequencies for Dlink card



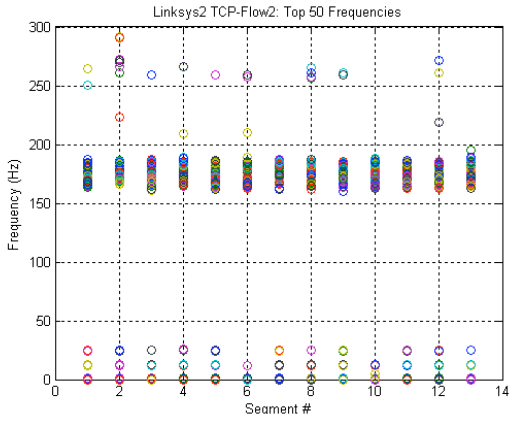
(d) (e)

(c)

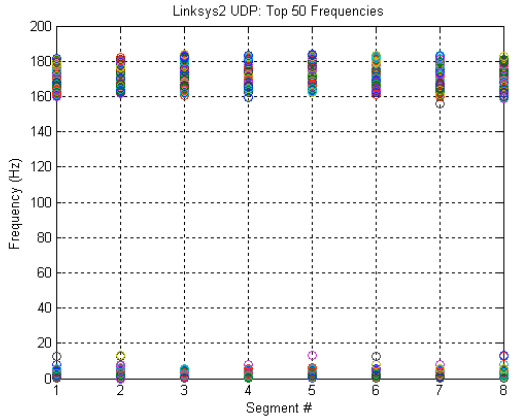
Figure 46 Top 50 frequencies for Linksys1



(a)

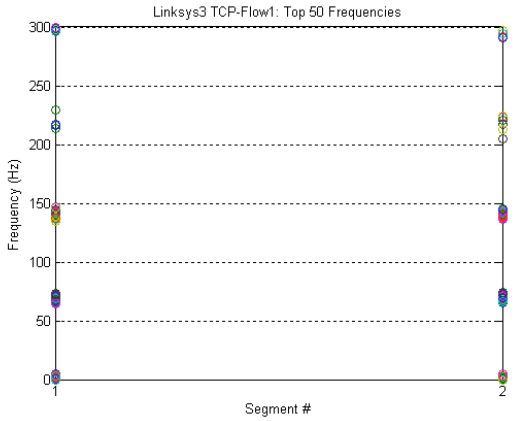


(b)

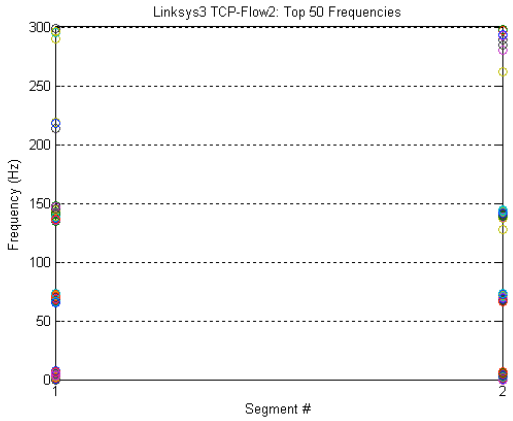


(c)

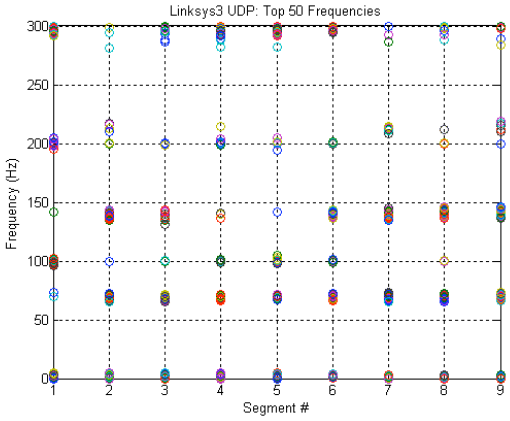
Figure 47 Top 50 frequencies for Linksys2



(a)

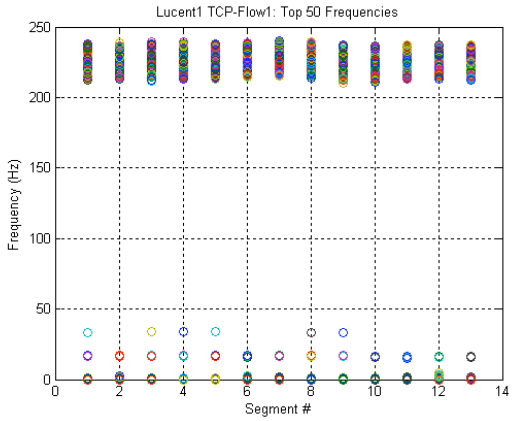


(b)

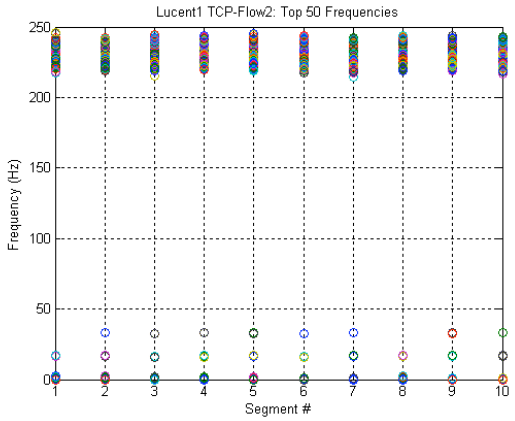


(c)

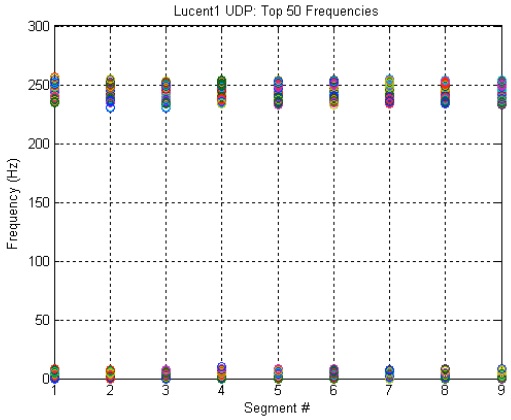
Figure 48 Top 50 frequencies for Linksys3



(a)

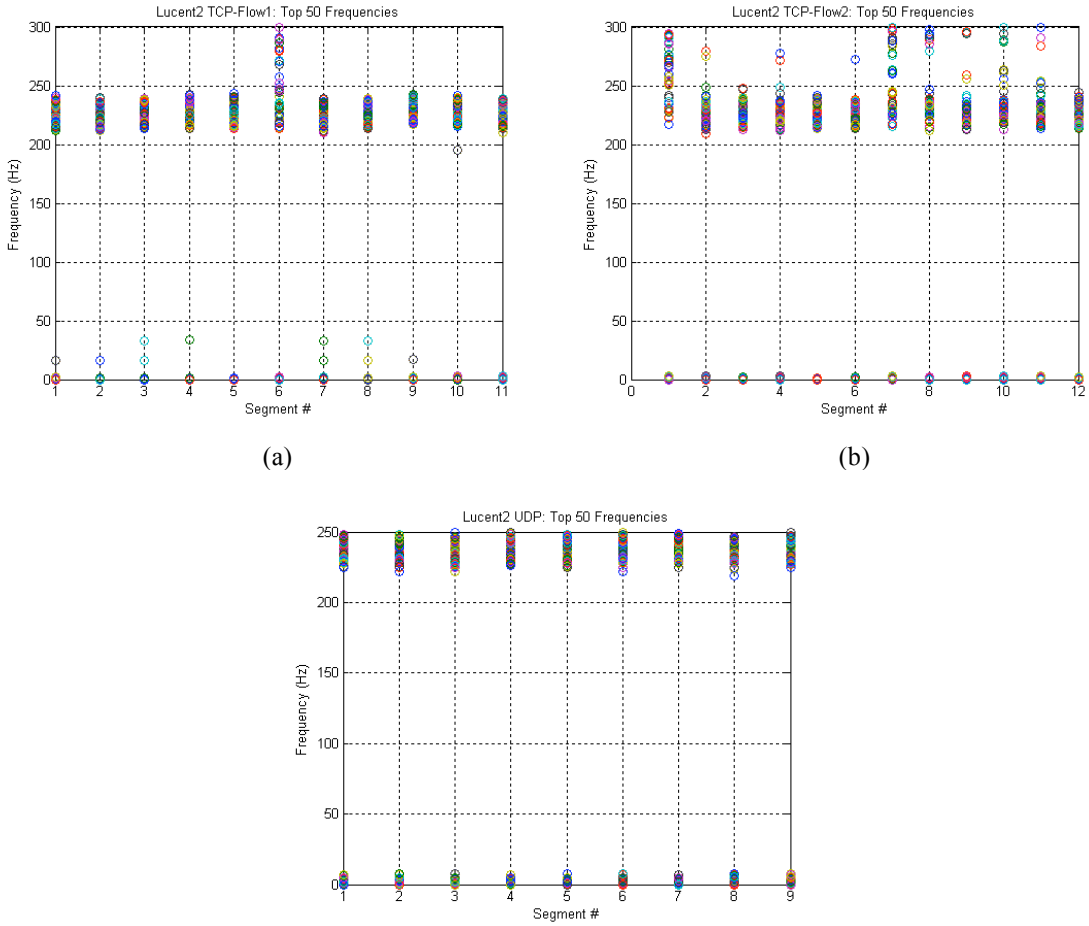


(b)



(c)

Figure 49 Top 50 frequencies for Lucent1



(a) (b)

(c)

Figure 50 Top 50 frequencies for Lucent2

APPENDIX H: RATE SWITCHING SPECTRAL PROFILE

This appendix illustrates the representative spectral profile $F_{\mathbf{R}} = \{f_1, f_2, f_3, \ldots f_{50}\}$ of each traffic type per card for the evaluation of the rate switching mechanism.

Table 45 Spectral Profile F_R for UDP flow

	Dlink	Linksys1	Linksys2	Linksys3	Lucent1	Lucent2
f_1	0.58477	1.1695	0.58477	0.58477	0	0
f_2	1.1695	1.7543	1.1695	1.1695	0.58477	0.58477
f_3	1.7543	2.3391	1.7543	1.7543	1.1695	1.1695
f_4	2.3391	2.9238	2.3391	2.3391	1.7543	1.7543
f_5	2.9238	3.5086	2.9238	2.9238	2.3391	2.3391
f_6	3.5086	4.0934	3.5086	3.5086	2.9238	2.9238
f_7	4.0934	4.6781	4.0934	4.0934	3.5086	3.5086
f_8	4.6781	5.2629	4.6781	66.079	4.0934	4.0934
f_9	5.2629	5.8477	5.2629	66.664	4.6781	4.6781
f_{10}	5.8477	8.1868	5.8477	67.248	5.2629	6.4324
f_{11}	13.45	160.23	160.81	67.833	5.8477	7.0172
f_{12}	160.81	160.81	161.98	68.418	6.4324	224.55
f_{13}	162.57	161.4	162.57	69.003	7.0172	225.14
f_{14}	163.74	161.98	163.15	69.587	7.602	225.72
f_{15}	164.32	162.57	163.74	70.172	230.4	227.47
f_{16}	164.9	163.15	164.32	70.757	231.57	228.06
f_{17}	165.49	163.74	164.9	71.342	233.91	228.64
f_{18}	166.07	164.32	165.49	71.926	234.49	229.23
f_{19}	166.66	164.9	166.07	72.511	235.08	229.81
f_{20}	167.24	165.49	166.66	98.826	235.66	230.4
f_{21}	167.83	166.07	167.24	99.411	236.25	230.98
f_{22}	168.41	166.66	167.83	99.995	236.83	231.57
f_{23}	169	167.24	168.41	100.58	237.42	232.15
f_{24}	169.58	167.83	169	101.16	238	232.74
f_{25}	170.17	168.41	169.58	136.25	238.59	233.32
f_{26}	170.75	169	170.17	136.84	239.17	233.91
f_{27}	171.34	169.58	170.75	137.42	239.75	234.49
f_{28}	171.92	170.17	171.34	138.59	240.34	235.08
f_{29}	172.51	170.75	171.92	139.17	240.92	235.66
f_{30}	173.09	171.34	172.51	139.76	241.51	236.25
f_{31}	173.68	171.92	173.09	140.34	242.09	236.83
f_{32}	174.26	172.51	173.68	140.93	242.68	237.42
f_{33}	174.85	173.09	174.26	141.51	243.26	238
f_{34}	175.43	173.68	174.85	142.1	243.85	238.59
f_{35}	176.02	174.26	175.43	142.68	244.43	239.17
f_{36}	176.6	174.85	176.02	143.27	245.02	239.75
f_{37}	177.18	175.43	176.6	199.41	245.6	240.34
f_{38}	177.77	176.02	177.18	199.99	246.19	240.92
f_{39}	178.35	176.6	177.77	200.58	246.77	241.51
f_{40}	178.94	177.18	178.35	201.16	247.36	242.09
f_{41}	179.52	177.77	178.94	294.14	247.94	242.68
f_{42}	180.11	178.35	179.52	294.72	248.53	243.26
f_{43}	180.69	178.94	180.11	295.31	249.11	243.85
f_{44}	181.28	179.52	180.69	295.89	249.7	244.43
f_{45}	181.86	180.11	181.28	296.48	250.28	245.02
f_{46}	182.45	180.69	181.86	297.06	250.87	245.6
f_{47}	183.03	181.28	182.45	297.65	251.45	246.19
f_{48}	183.62	181.86	183.03	298.23	252.03	246.77
f_{49}	185.37	182.45	183.62	298.82	252.62	247.36
f_{50}	185.96	183.03	184.2	299.4	253.2	248.53

Table 46 Spectral Profile for TCP-Flow1

	Dlink	Linksys1	Linksys2	Linksys3	Lucent1	Lucent2
f_1	0	0	0	0	0	0
f_2	0.58477	0.58477	0.58477	0.58477	0.58477	0.58477
f_3	1.1695	1.1695	1.1695	1.1695	1.1695	1.1695
f_4	1.7543	1.7543	1.7543	1.7543	1.7543	1.7543
f_5	2.3391	2.3391	2.3391	2.3391	2.3391	213.44
f_6	11.111	4.6781	3.5086	2.9238	16.374	214.61
f_7	11.695	10.526	11.695	3.5086	16.958	215.78
f_8	12.28	11.111	150.29	4.0934	212.86	216.36
f_9	156.72	11.695	150.87	4.6781	213.44	216.95
f_{10}	158.47	12.28	152.04	64.909	214.03	217.53
f_{11}	159.06	161.4	152.62	65.494	214.61	218.12
f_{12}	159.64	161.98	155.55	66.079	215.19	218.7
f_{13}	160.23	163.15	156.13	66.664	215.78	219.29
f_{14}	160.81	164.9	156.72	67.248	216.36	219.87
f_{15}	161.4	165.49	157.3	67.833	216.95	220.46
f_{16}	161.98	166.07	157.89	68.418	217.53	221.04
f_{17}	162.57	166.66	158.47	69.003	218.12	221.63
f_{18}	163.15	167.24	159.64	69.587	218.7	222.21
f_{19}	163.74	167.83	160.23	70.172	219.29	222.8
f_{20}	164.32	168.41	160.81	70.757	219.87	223.38
f_{21}	164.9	169	161.4	71.342	220.46	223.97
f_{22}	166.07	169.58	161.98	71.926	221.04	224.55
f_{23}	166.66	170.17	162.57	72.511	221.63	225.14
f_{24}	167.24	170.75	163.15	73.096	222.21	225.72
f_{25}	167.83	171.34	163.74	135.08	222.8	226.31
f_{26}	168.41	171.92	164.32	136.84	223.38	226.89
f_{27}	169	172.51	164.9	137.42	223.97	227.47
f_{28}	169.58	173.09	165.49	138.01	224.55	228.06
f_{29}	170.17	173.68	166.07	138.59	225.14	228.64
f_{30}	170.75	174.26	166.66	139.17	225.72	229.23
f_{31}	171.34	174.85	167.24	139.76	226.31	229.81
f_{32}	171.92	175.43	167.83	140.34	226.89	230.4
f_{33}	172.51	176.02	168.41	140.93	227.47	230.98
f_{34}	173.68	176.6	169	141.51	228.06	231.57
f_{35}	174.85	177.18	169.58	142.1	228.64	232.15
f_{36}	175.43	177.77	170.17	142.68	229.23	232.74
f_{37}	176.02	178.35	170.75	143.27	229.81	233.32
f_{38}	247.36	178.94	171.34	143.85	230.4	233.91
f_{39}	258.47	179.52	171.92	144.44	230.98	234.49
f_{40}	261.39	180.11	172.51	146.19	231.57	235.08
f_{41}	267.24	180.69	173.09	146.78	232.15	235.66
f_{42}	267.82	181.28	173.68	213.44	232.74	236.25
f_{43}	268.41	181.86	174.26	216.36	233.32	236.83
f_{44}	270.75	182.45	174.85	216.95	233.91	237.42
f_{45}	271.92	183.03	175.43	229.23	234.49	238
f_{46}	274.84	183.62	176.02	296.48	235.08	238.59
f_{47}	293.55	184.2	176.6	297.06	235.66	239.17
f_{48}	297.06	184.79	177.77	298.23	236.25	239.75
f_{49}	297.65	185.37	178.35	298.82	236.83	240.92
f_{50}	298.23	187.71	178.94	299.4	238.59	243.26

Table 47 Spectral Profile for TCP-Flow2

	Linksys1	Linksys2	Linksys3	Lucent1	Lucent2
f_1	0	0	0	0	0
f_2	0.58477	0.58477	0.58477	0.58477	0.58477
f_3	1.1695	1.1695	1.1695	1.1695	1.1695
f_4	1.7543	1.7543	1.7543	1.7543	1.7543
f_5	11.695	4.6781	2.3391	2.3391	2.3391
f_6	12.28	11.695	2.9238	2.9238	213.44
f_7	12.865	12.28	3.5086	16.374	214.03
f_8	24.56	12.865	4.0934	16.958	214.61
f_9	25.145	163.15	4.6781	217.53	215.19
f_{10}	161.98	163.74	5.2629	218.12	215.78
f_{11}	162.57	164.32	5.8477	220.46	216.36
f_{12}	163.15	164.9	7.0172	221.04	216.95
f_{13}	163.74	165.49	7.602	221.63	218.12
f_{14}	165.49	166.07	65.494	222.21	218.7
f_{15}	166.07	166.66	66.664	222.8	219.29
f_{16}	166.66	167.24	67.248	223.38	219.87
f_{17}	167.24	167.83	67.833	223.97	220.46
f_{18}	167.83	168.41	68.418	224.55	221.04
f_{19}	168.41	169	69.003	225.14	221.63
f_{20}	169	169.58	69.587	225.72	222.21
f_{21}	169.58	170.17	70.172	226.31	222.8
f_{22}	170.17	170.75	70.757	226.89	223.38
f_{23}	170.75	171.34	71.342	227.47	223.97
f_{24}	171.34	171.92	71.926	228.06	224.55
f_{25}	171.92	172.51	72.511	228.64	225.14
f_{26}	172.51	173.09	73.096	229.23	225.72
f_{27}	173.09	173.68	135.08	229.81	226.31
f_{28}	173.68	174.26	135.67	230.4	226.89
f_{29}	174.26	174.85	136.25	230.98	227.47
f_{30}	174.85	175.43	136.84	231.57	228.06
f_{31}	175.43	176.02	137.42	232.15	228.64
f_{32}	176.02	176.6	138.01	232.74	229.23
f_{33}	176.6	177.18	138.59	233.32	229.81
f_{34}	177.18	177.77	139.17	233.91	230.4
f_{35}	177.77	178.35	140.93	234.49	230.98
f_{36}	178.35	178.94	141.51	235.08	231.57
f_{37}	178.94	179.52	142.1	235.66	232.15
f_{38}	179.52	180.11	142.68	236.25	232.74
f_{39}	180.11	180.69	144.44	236.83	233.32
f_{40}	180.69	181.28	145.02	237.42	233.91
f_{41}	181.28	181.86	145.61	238	234.49
f_{42}	181.86	182.45	147.36	238.59	235.08
f_{43}	182.45	183.03	147.95	239.17	235.66
f_{44}	183.03	183.62	213.44	239.75	236.25
f_{45}	183.62	184.2	218.12	240.34	236.83
f_{46}	184.2	184.79	218.7	240.92	237.42
f_{47}	184.79	185.37	290.04	242.09	238.59
f_{48}	185.37	185.96	295.31	242.68	240.34
f_{49}	185.96	187.71	295.89	245.6	240.92
f_{50}	186.54	188.3	298.82	246.19	244.43

REFERENCES

[1] IEEE 802.11 specification, http://standards.ieee.org/getieee802/802.11.html, accessed March 14, 2005.

[2] IEEE 802.11i specification, http://standards.ieee.org/getieee802/802.11.html, accessed March 14, 2005.

[3] Nikita Borisov, Ian Golberg, and David Wagner, "Intercepting mobile communications: The insecurity of 802.11," MOBICOM 2001.

[4] Jesse Walker, "Unsafe at any key size: an analysis of the WEP encapsulation," Tech. Rep. 00/362, IEEE 802.11 Committee, March 2000, DocumentHolder/0-362.zip, http://grouper.ieee.org/groups/802/11/Documents/.

[5] Arunesh Mishra and William Arbaugh, "Your 802.11 Wireless Network has No Clothes," IEEE Wireless Communications Magazine, December 2002 .

[6] Fluhrer, S., I. Mantin, and A. Shamir, "Weaknesses in the key schedule algorithm of RC4," In *Proc. 4th Annual Workshop on Selected Areas of Cryptography, 2001*.

[7] The Definitive Guide to Wireless WarXing, teknik.ekitap.gen.tr/TDGTW-WarXing.html, accessed March 14, 2005.

[8] J. Bellado, "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions," Proceedings for the USENIX Security Symposium, August 2003.

[9] Mike Lynn and Robert Baird, "Advanced 802.11 Attack," BlackHat Briefings, July 2002, http://www.blackhat.com/html/bh-usa-02/bh-usa-02-speakers.html #bard.

[10] Bob Fleck and Jordan Dimov, "Wireless Access Points and ARP Poisoning," http://www.barbedwiretech.com/Technology/wp-pdf/BW-wifi_ArpPoison.pdf, accessed March 14, 2005.

[11] Raheem Beyah, Shantanu Kangude, George Yu, Brian Strickland, and John Copeland. "Rogue Access Point Detection using Temporal Traffic Characteristics." *Proceedings of IEEE GLOBECOM 2004, December 2004.*

[12] Joel Branch, Nick Petroni Jr., Leendert Van Doorn, and David Safford, "Autonomic 802.11 Wireless LAN Security Auditing," IEEE Security & Privacy, May/June 2004, pp. 56-65.

[13] WaveLink, "Rogue Access Point Detection," www.wavelink.com/downloads/pdf/ wlmobilemanager wp_rogueap.pdf, accessed March 14, 2005.

[14] Cisco, "Detecting Rogue 802.11 Access Points within the Enterprise", http://winfingerprint.sourceforge.net/presentations/APTools.ppt/, accessed March 14, 2005.

[15] http://www.computerworld.com/mobiletopics/mobile/story/0,10801,72065,00.html, accessed March 14, 2005.

[16] Joshua Wright, "Detecting Wireless LAN MAC Address Spoofing," http://home.jwu.edu/jwright/papers/wlan-mac-spoof.pdf, accessed March 14, 2005.

[17] ReefEdge, http://www.tribecaexpress.com/reefedge.htm, accessed March 14, 2005.

[18] AirDefense, www.airdefense.net, accessed March 14, 2005.

[19] AirMagnet, http://www.airmagnet.com/, accessed March 14, 2005.

[20] WiMetrics, www.wimetrics.com, accessed March 14, 2005.

[21] iPass, www.ipass.com/services/servicesdeviceid.html, accessed March 14, 2005.

[22] "Cellular Companies Fight Fraud", www.decodesystems.com/mt/97dec/, accessed March 14, 2005.

[23] Jeyanthi Hall, Michel Barbeau, and Evangelos Kranakis, "Detection of Transient in Radio Frequency Fingerprinting using Signal Phase," Internet and Information Technology (CIIT), St. Thomas, US Virgin Islands, November 2004.

[24] Tadayoshi Kohno, Andre Briodo, KC Claffy, "Remote Physical Device Fingerprinting, " IEEE Transactions on Dependable and Secure Computing, vol. 2, no. 2, pp. 93-108, April-June 2005.

[25] Yarochkin Fyodor, "Remote OS detection via TCP/IP Stack FingerPrinting." October 18, 1998. URL: http://www.insecure.org/nmap/nmap-fingerprinting-article.txt.

[26] Ofir Arkin and Fyodor Yarochkin, "Xprove v2.0: A Fuzzy Approach to Remote Active Operating System Fingerprinting," August 2, 2002, URL: http://www.sys-security.com/archive/papers/Xprobe2.pdf.

[27] Arunesh Mishra, Minho Shin, and William Arbaugh, "An Empirical Analysis of the IEEE 802.11 MAC Layer Handoff Process," ACM Computer Communications Review, vol. 33, no. 2, pp. 93-102, 2003.

[28] Ishwar Ramani and Stefan Savage, "SyncScan: Practical Fast Handoff for 802.11 Infrastructure Networks," in Proceedings of IEEE INFOCOM, March 2005.

[29] M. Lacaga, M. Manshaei, and T. Turletti, "IEEE 802.11 Rate Adaptation: A Practical Approach," ACM/IEEE MSWIM, Venice, Italy, October 2004.

[30] P. Chevillat, J. Jelitto, A. Noll Barreto, and H. L. Truong, "A Dynamic Link Adaptation Algorithm for IEEE 802.11a Wireless LANs," in *Proc. IEEE ICC 2003*, Anchorage, AK, May 2003, pp. 1141-1145.

[31] GigaMobile, "Application-directed automatic 802.11 rate control," https://doc.freeband.nl/dscgi/ds.py/Get/File-28445/GigaMobile-D3.16.pdf, accessed December 5, 2005.

[32] Ad Kamerman and Leo Monteban, "WaveLAN-II: a high-performance Wireless LAN for the Unlicensed Band," *Bell Labs Technical Journal*, vol.2, no.3, pp.118-133, Aug. 1997.

[33] Sunwoong Choi, Kihong Park, Chong-kwon Kim, "On the Performance Characteristics of WLANs: Revisited," *SIGMETRICS '05*, June 6-10, 2005, Banff, Alberta, Canada.

[34] "Agere's WiFi chipset reaches 150Mbit/s", www.electronicsweekly.com/Article 5144 .html, accessed March 14, 2005.

[35] Chen-Mou Cheng, H.T. Kung, and Koan-Sin Tan, "Use of spectral analysis in defense against DoS attacks," in Proceedings of the IEEE GLOBECOM, Taipei, Taiwan, 2002.

[36] Alefiya Hussain, John Heidemann, Christos Papadopoulos, "Identification of repeated attacks using network traffic forensics," Technical Report ISI-TR-2003-577b, USC/Information Sciences Institute, August, 2003.

[37] Craig Partridge et al., "Using Signal Processing to Analyze Wireless Data Traffic," *ACM Workshop on Wireless Security (WiSe),* Atlanta, GA, USA, September 28, 2002.

[38] James McClellan, Ronald Schafer, and Mark Yoder, *Signal Processing First*, Prentice Hall, 2003.

[39] Oppenheim, A.V., and R.W. Schafer, *Discrete-Time Signal Processing*, Prentice-Hall, 1989, pp. 730-742.

[40] Signal Processing Toolbox, http://www.mathworks.com/access/helpdesk/help/ toolbox/ signal/, accessed March 1, 2006.

[41] The linux-wlan™ Project, http://www.linux-wlan.org/, accessed March 14, 2005.

[42] http://www.tcpdump.org/, accessed March 14, 2005.

[43] W. Richard Stevens, *Unix Network Programming, Volume 1.* Upper Saddle River, NJ: Prentice Hall PTR 1998.